Office of Technology Assessment

Congressional Board of the 97th Congress

TED STEVENS, *Alaska, Chairman*

MORRIS K. UDALL, *Arizona, Vice Chairman*

Senate

ORRIN G. HATCH
Utah

CHARLES McC. MATHIAS, JR.
Maryland

EDWARD M. KENNEDY
Massachusetts

ERNEST F. HOLLINGS
South Carolina

HOWARD W. CANNON
Nevada

House

GEORGE E. BROWN, JR.
California

JOHN D. DINGELL
Michigan

LARRY WINN, JR.
Kansas

CLARENCE E. MILLER
Ohio

COOPER EVANS
Iowa

JOHN H. GIBBONS
(Nonvoting)

Advisory Council

CHARLES N. KIMBALL, *Chairman*
Midwest Research Institute

JEROME B. WIESNER, *Vice Chairman*
Massachusetts Institute of Technology

EARL BEISTLINE
University of Alaska

CHARLES A. BOWSHER
General Accounting Office

CLAIRE T. DEDRICK
California Land Commission

JAMES C. FLETCHER
University of Pittsburgh

S. DAVID FREEMAN
Tennessee Valley Authority

GILBERT GUDE
Library of Congress

CARL N. HODGES
University of Arizona

RACHEL McCULLOCH
University of Wisconsin

FREDERICK C. ROBBINS
Institute of Medicine

LEWIS THOMAS
Memorial Sloan-Kettering Cancer Center

Director

JOHN H. GIBBONS

This is an OTA Background Paper that has neither been reviewed nor approved by the Technology Assessment Board

J952-8

Selected Electronic Funds Transfer Issues

Privacy, Security, and Equity

Background Paper

OTA Background Papers are documents containing information that supplements formal OTA assessments or is an outcome of internal exploratory planning and evaluation. The material is usually not of immediate policy interest and does not present options for Congress to consider.

CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, D.C. 20510

Library of Congress Catalog Card Number 82-600524

For sale by the Superintendent of Documents,
U.S. Government Printing Office, Washington, D.C. 20402

Foreword

This background paper on selected electronic funds transfer (EFT) issues is one of four components of the OTA assessment of Societal Impacts of National Information Systems. It should be read along with the September 1981 OTA report on *Computer-Based National Information Systems: Technology and Public Policy Issues*, which provides the larger context for understanding EFT-related public policy questions.

The Senate Committee on the Judiciary, one of the original requesting committees, indicated an interest in possible implications of EFT for privacy, security, and equity, among other issue areas. In response, OTA initiated a preliminary analysis of relevant EFT developments since the completion of the work of the National Commission on Electronic Funds Transfer. Several working papers were prepared by OTA staff and contractors. These were reviewed by a special advisory panel on EFT representing financial, business, academic, and consumer interests. On the basis of that review, a revised and integrated paper was prepared.

OTA appreciates the participation of the advisory panelists, external reviewers, and others who helped bring this background paper to fruition. It is, however, solely the responsibility of OTA, not of those who so ably advised and assisted us in its preparation.

John H. Gibbons

JOHN H. GIBBONS
Director

Advisory Panel Members for the EFT Study*

Kent W. Colton, *Chairman*
Professor of Public Management, Brigham Young University

Wayne I. Boucher
Center for Futures Research
University of Southern California

Roland R. Eppley, Jr.**
President
Eastern States Bank Card Association

John Fisher
Senior Vice President
BANC ONE

Maurice W. Gregg
Senior Vice President for Finance
The Gap Stores, Inc.

Jeremiah S. Gutman
Attorney at Law
Levy, Gutman, Goldberg & Kaplan

Michael A. Levine
Vice President
Citibank

Allen H. Lipis
President
Electronic Banking, Inc.***

John McDonnell, Jr.
Eastern Regional Manager
Tymnet, Inc.

Susan Nycum
Attorney at Law
Gaston Snow & Ely Bartlett

William H. Riley
Attorney at Law
Cunningham, Blackburn, VonSeggern,
Livingston, Francis & Riley

James Rule
Professor of Sociology
State University of New York at Stony Brook

Jerome Svigals
IBM Corp.

Willis H. Ware
Senior Computer Specialist
The Rand Corp.

Robert C. Zimmer
Counsel
Electronic Money Council

NOTE: The advisory panel provided advice and critique throughout the study, but does not necessarily approve, disapprove, or endorse the report, for which OTA assumes full responsibility.

*Panelist affiliations at time of appointment to panel.
**Later represented by Howard Mandelbaum, Manufacturers Hanover Trust Co.
***Served as a panelist until February 1980.

OTA Electronic Funds Transfer Project Staff

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

Sam Hale, *Interim Program Manager,*
*Communication and Information Technologies**

Fred B. Wood, *Project Director*
Zalman A. Shavell, *EFT Study Director*
Jean E. Smith, *Analyst*
Daniel Kevin, *Analyst*
Fred W. Weingarten, *Senior Analyst*
Elizabeth A. Emanuel, *Administrative Assistant*
Shirley Gayheart, *Secretary*
Teri Miles, *Secretary***
Jeanette Contee, *Wordprocessor*

Contractors

Vary T. Coates, Consultant
Renee G. Ford, Tifford Producers Ltd.
Allen H. Lipis, Electronic Banking, Inc.
John B. Benton and Donald C. Leonard, ICS Group, Inc.
John L. King, Rob Kling, and Kenneth L. Kraemer,
The Irvine Research Corp.
Fred M. Greguras, Kutak, Rock, & Huie

OTA Publishing Staff

John C. Holmes, *Publishing Officer*

John Bergling Kathie S. Boss Debra M. Datcher Joe Henson

*Since March 1981; Stephen E. Doyle served as Program Manager through February 1981.
**Until June 1981.

Acknowledgments

The following individuals also contributed as reviewers during the course of this study:

Louise Becker
Congressional Research Service

R. Lamar Brantley
U.S. League of Savings Associations

Jim Embersit
Office of Comptroller of the Currency

Henry v. Z. Hyde, Jr.
Electronic Funds Transfer Association (formerly)

Donald A. Marchand
University of South Carolina at Columbia

Elliott C. McEntee
Federal Reserve System

Donn B. Parker
SRI International

Henry M. Polmer
Bell, Boyd & Lloyd

Lawrence Robertson
National Telecommunications and Information Administration (formerly)

William H. Robinson, Sr.
Wilmington Savings Fund Society

Scott Sacks
Federal Trade Commission

Contents

Chapter	*Page*
1. Summary	3
2. Electronic Funds Transfer Technologies and Services	9
Chapter Summary	9
Introduction	9
Automated Teller Machines	10
Point-of-Sale	12
Credit Card Authorization and Check Validation	13
Debit Cards	13
Telephone Bill Payment	14
Wire Transfer	15
Check Truncation	15
Automated Clearinghouses	15
3. Competitive and Regulatory Environment of Electronic Funds Transfer	19
Chapter Summary	19
The Payments System	19
Providers and Regulators of Payment Services	20
Existing and Proposed Laws	21
Interstate EFT Services	23
Key Actors in EFT Development	24
4. Privacy in Electronic Funds Transfer	29
Chapter Summary	29
What is Privacy?	30
Privacy in Financial Transactions	30
What Constitutes a Violation of Privacy?	31
EFT and Privacy	32
The Economics of EFT Privacy	35
Concern About Government Surveillance	35
Legal Protection of Privacy in EFT	36
5. Security in Electronic Funds Transfer	45
Chapter Summary	45
Security in Payment Systems	46
Types of EFT Crime or Breaches of Security	48
How Serious is EFT Crime at Present?	49
Technology and Techniques for Increased EFT Security	50
Security and Public Discussion	52
Relationship of Security to Privacy and Equity	53
6. Equity in Electronic Funds Transfer	57
Chapter Summary	57
What is Equity?	58
Equity in Payment Systems	59
EFT Equity and the Socially Disadvantaged	59
The Poor	60
The Elderly	60
Women	61

Page
Racial/Ethnic Groups . . . 61
The Handicapped or Disabled . . . 61
Transitional Groups Without Recognized Financial Status . . . 61
The General Public as Consumers of Financial Services . . . 62
The Knowledge to Choose . . . 62
The Preservation of Options . . . 63
The Economics of Payment Systems . . . 64
Personal Money Management . . . 65
Liability . . . 66
Customer Vulnerability to Errors . . . 66
In Conclusion . . . 66

Appendixes

A. Other Questions and Issues Concerning Electronic Funds Transfer . 71
Appendix Summary . . . 71
EFT and the Structure of the Financial Services Industry . . . 71
EFT and the National Welfare . . . 73
The Government Role in EFT . . . 74
B. List of Working Papers . . . 77

LIST OF TABLES

Table No. *Page*
1. Financial Services—Non-EFT and EFT . . . 9
2. EFT Services and Technologies . . . 11
3. Point-of-Sale Services . . . 12
4. Key Institutional Actors in EFT Development . . . 25
5. EFT Services: Public Awareness, Availability, Usage, and Interest . . . 26
6. Comparison of NCEFT Recommendations on Privacy With Present Status of Existing Proposed Legislation . . . 37
7. Major Categories of Threats to EFT Security . . . 51
A-1. A Comparison of EFT Threat Levels by Source of Threat . . . 73

FIGURE

Figure No. *Page*
1. The Tangled Web of Banking Regulation . . . 22

Chapter 1
Summary

BEST AVAILABLE COPY

Chapter 1

Summary

Introduction

Electronic funds transfer (EFT) provides an alternative method of paying for goods and services and making a wide range of financial transactions that will increasingly challenge currency and checks as a dominant payment system. EFT is a cluster of technologies that allow the execution of financial transactions by electronic messages without the necessity of a paper instrument of exchange. The messages substitute for an exchange of currency or a signed check. The term EFT has also come to include electronic transfer of information critical to such transactions without an immediate transfer of funds; for example, credit authorization or check validation by telecommunication.

Some EFT systems are used for transfers between large organizations or institutions. For instance, automated clearinghouses (ACHs) receive, sort, and redistribute financial information that instructs participating banks to debit and credit accounts at a specified time. ACH services are used by some organizations for direct deposit of wages to employee accounts in many different banks.

Other EFT systems provide services to and for individual consumers. Automated teller machines (ATMs) are now widely available in many communities for making deposits or withdrawing funds 24 hours a day. Other consumer-oriented EFT technologies include point-of-sale terminals and telephone bill payer systems. Most EFT systems involve computers, telecommunication links, and automated data files. (See ch. 2 for detailed discussion of EFT technologies and services.)

Since EFT is a new and evolving technology, whose full impacts are unknown, it has given rise to a number of concerns. This paper focuses on the issues of user privacy, system security, and consumer equity in the use of EFT systems and services. Other EFT-related issues, such as competitive implications of electronic interstate banking and shared EFT networks, vulnerability of EFT to national security threats, impacts of EFT on employment, and the Federal Government role in EFT, are outside the scope of this preliminary analysis but are discussed briefly in appendix A.*

One major incentive for financial institutions in the move to EFT is the desire to reduce the growing burden of check handling and processing. The cost of processing checks is estimated at approximately $7.5 billion annually and is increasing rapidly because of rising labor costs and postage fees and the expanding volume of checks (about 5 percent more checks each year). The push for EFT is also a response to the dynamic interaction of the recent economic environment, increasing consumer sophistication, and deregulation of the banking and thrift industries. (See ch. 3 for a discussion of the competitive and regulatory environment of EFT.)

A number of factors appear to be accelerating the rate of EFT development. As a result of deregulation, the distinctions between the services offered by banks, thrift institutions, and other financial institutions are breaking down. Moreover, competing services are being marketed by nondepository institutions (e.g., securities brokers, credit card companies, and retailers). EFT makes it easier for firms to compete in financial services markets that were previously protected

*See also, the OTA report *Computer-Based National Information Systems: Technology and Public Policy Issues*, OTA-CIT-146 (Washington, D.C.: Government Printing Office, September 1981).

by regulatory boundaries. As in other areas of our economy, advancing EFT technology is contributing to de facto deregulation of markets.

In addition, financial institutions are no longer able to readily subsidize the cost of the paper-based payments system. Historically, financial institutions could more than cover the cost from earnings accruing as a result of the margin between regulated interest rates paid on deposits and market interest rates. Higher interest rates and the increasing demand by consumers to earn market rates of interest have reduced the availability of low-cost funds to subsidize paper-based transactions. Furthermore, the Federal Reserve is now required to explicitly charge for check-clearing services. Thus, EFT is used by firms in part to help offset these cost pressures as well as to counter general inflationary pressures.

In sum, EFT is increasingly viewed as an important part of the competitive and cost-containment strategies of institutions competing (or planning to compete) in the financial services markets. Projections of EFT deployment are still very rough at best, and have been badly off the mark in the past. But recent developments suggest that within the next two decades, EFT will transform the way many Americans carry out their day-to-day commercial activities and personal monetary transactions.

Privacy

Three principal concerns about EFT privacy have arisen: 1) the extent to which personal data in EFT systems are or might be disclosed to third parties by financial institutions; 2) the possibility of Government or private surveillance through EFT systems and data files; and 3) the right of consumers to see, challenge, and correct personal data in EFT systems that might be used, for example, to refuse them credit or in other disadvantageous ways.

With increased use of EFT there will be a large number of points at which traditional norms of privacy could be violated. More EFT terminals will be online, making electronic surveillance a more credible possibility. Single statement reporting of all kinds of financial transactions will become common; more data will be aggregated and thus easier to access. There could be broader and swifter dissemination of inaccurate data. Even if customer correction of data is facilitated, it will be more difficult for corrections to catch up with and replace faulty information.

In 1977, both the Privacy Protection Study Commission and the National Commission on Electronic Funds Transfer (NCEFT) recognized that EFT privacy concerns could be especially strong. NCEFT devoted 19 recommendations to means of protecting privacy.

Only a few of the NCEFT recommendations are reflected in the two EFT-related laws enacted since 1977—the Electronic Funds Transfer Act of 1978 (and Federal Reserve Regulation E) and the Right to Financial Privacy Act of 1978. For example, the use of EFT systems for surveillance purposes is not covered by existing legislation, but would be tightly restricted by the proposed privacy of EFT bill introduced in the 96th Congress. Disclosure of EFT information to third parties is addressed only minimally by the EFT Act of 1978. The proposed privacy of EFT and fair financial information practices bills would provide more detailed conditions and restrictions on third party disclosure. Even so, these proposed conditions are not as restrictive as some customers would prefer, and neither of these bills was enacted by the 96th Congress.

Thus, the needs identified by NCEFT for more comprehensive EFT privacy protection, whether through new legislation, modification of existing law, administrative procedures and regulations, industry standards, or some combination, are still largely unmet.

Security

Security means the protection of the integrity of EFT systems and their information from illegal or unauthorized access and use. Although the loss per theft appears to be greater than for paper-based payment systems, there is no real evidence that EFT systems to date have resulted in a higher than average crime rate. Why, then, is the security of EFT systems an important public concern and potentially a major policy issue? In comparison with other payment systems, EFT appears to have some additional vulnerabilities. For example:

- EFT systems have many points of access where transactions can be affected in unauthorized ways because of direct customer involvement with the dynamics of the systems, the use of telecommunication lines, and the ways in which data are aggregated and transmitted among and between sites and institutions.
- EFT crime is often difficult to detect because funds/data can be removed or manipulated by instructions hidden in complex computer software; the dynamics of the criminal action may be understood by only a few experts within the institution.
- EFT crime offers a sporting element, or intellectual challenge, that perhaps is as enticing to some as the opportunity for financial gain.
- It is possible, in theory, for large banks of data to be destroyed by remote agents, creating the opportunity for maliciousness, extortion, blackmail, or terrorism.
- EFT systems reduce the effectiveness of—or eliminate altogether—some of the traditional methods of controlling and auditing access to financial accounts.

The level of EFT security violations is difficult to assess at present because there is underreporting of EFT crime, a paucity of information about EFT security, and a lack of informed public discussion. While there is a danger that giving these problems higher visibility through public discussion may at first exacerbate them, the public is entitled to know what risks they are exposed to in using EFT services. Furthermore, both law enforcement agents and financial institutions would benefit by sharing information about vulnerabilities, defense strategies, and security-enhancing technologies.

Some believe that effective technology and sound management procedures exist to adequately assure EFT security, though even present technology and procedures are not all widely used. Their use varies among institutions. There is as yet no clear and consistent set of industrywide security standards for protecting computer systems.

Better information about EFT security would allow Congress and State legislatures to assess more effectively the possible need for new legislation and/or regulations.

Equity

The concept of equity includes the principles that individuals, groups, and organizations should be afforded access to necessary financial services; that the range of financial choice, rights, and benefits that consumers now enjoy should not be arbitrarily reduced; and that the rules and procedures for access to and choice of financial services should not be differentially reduced for certain population subgroups.

As long as EFT is one of an array of alternative payment systems or sets of financial services, it does not appear that its use will result in a necessary or significant loss of equity to any group in society. EFT delivers benefits to many customers, and these could be increased if technology designers and financial service managers were attentive to diverse human needs. For example, dispersed EFT devices could be tailored to the needs of the handicapped, and located to meet the needs of those whose mobility is limited. EFT offers important and obvious benefits in terms of customer convenience

and reduced costs and increased productivity for financial institutions (presumably for customers as well), and perhaps greater personal security for the user against crimes of violence and some kinds of privacy abuse.

However, to the extent that some forms of participation in EFT become mandatory or inescapable, or to the extent that EFT significantly displaces, reduces, or raises the costs of alternatives, some population subgroups could experience a loss of equity. Some people who choose not to deal with banks and other financial institutions could be forced to do so. People who for various reasons are poorly equipped to use EFT systems could have their access to financial services reduced. Some communities or neighborhoods could suffer a reduction in available financial services. Explicit public policies may need to be considered to preserve some level of conventional financial services if market and other forces move EFT to a dominant role.

Chapter 2

Electronic Funds Transfer Technologies and Services

BEST AVAILABLE COPY

Chapter 2

Electronic Funds Transfer Technologies and Services

Chapter Summary

Electronic funds transfer (EFT) consists of a group of technologies that allow financial transactions to be carried out electronically. Messages sent by several forms of telecommunication cause funds to be transferred from one financial account to another. The messages substitute for an exchange of currency or for a signed check that would bring about the same transfer. The term EFT has also come to include transfer of information critical to such transactions without an immediate transfer of funds; for example, authorization of credit or validation of checks by telecommunication. Although most EFT technologies are at most 15 years old, they are already having a significant impact on payment systems and on banks and other financial institutions. It is possible that within the next two decades EFT will transform the way Americans carry out their day-to-day commercial activities and personal monetary transactions.

Introduction

EFT is not one but several technologies, all requiring the processing and transmission of information by electronic means to effect an economic exchange and financial service. Some of these services (listed in table 1) are decentralized and are provided directly to the consumer at retail. They consist of transactions that may involve an individual, a provider of goods or services that are purchased by the individual, and one or more providers of financial services. In some cases, as in the use of an automated teller machine (ATM), the transfer is almost immediate. In others, value is conveyed by a paper instrument, such as a check, while the electronic service provides information to the recipient that good funds are being conveyed. For example, check verification services help eliminate uncertainty as to whether a check will be returned for lack of funds. Sometimes the consumer operates a machine that is used to provide an EFT service. In other cases, the consumer gains access to a service through an intermediary.

Table 1.—Financial Services—Non-EFT and EFT

I. Non-EFT financial transactions
- Currency
- Checks and magnetic coding of checks
- Credit card services

II. Consumer oriented/decentralized EFT services

A. Services that facilitate the transfer of information
- Check and credit authorization
- Check verification
- Check guarantee
- Account status inquiry

B. EFT services that involve direct money transfer
- Deposit
- Cash withdrawal
- Bill or loan payment
- Interaccount transfer
- Debit of transaction balance with overdraft privileges
- Credit purchase
- Cash advance

III. Institution oriented/centralized EFT services
- Direct deposit of payroll
- Preauthorized debit services
- Corporate cash management (including interbank and intrabank transfers
- Interbank settlements and clearings

SOURCE: Kent W. Colton, et al., *Electronic Funds Transfer Systems and Crime*, Public Systems Evaluation, Inc., February 1981 draft

91-217 O - 82 - 3 : QL 3

Other EFT services (listed in table 1) are more centralized and generally are used for transfers between financial institutions, or between these institutions and large-scale users, such as the U.S. Treasury. These are also referred to as wholesale services and include wire transfers and automated clearinghouses (ACHs). Some electronic transfers take place entirely within the computer of one bank. At times individuals will participate in wholesale services, but most will not do so routinely. These centralized services are largely invisible to the consumer, and chiefly affect relationships between institutions. However, there are times when data that are identifiable with a particular individual are handled by a wholesale service; e.g., the transmission of payroll through the ACH network.

Most EFT services involve computers, automated data files, telecommunication links, and access systems. To fulfill the obligations of financial institutions to their users, and to guard against mistakes, EFT services create transaction logs and audit trails. All promise, when fully implemented, to deliver substantial cost savings. In transferring funds between accounts or institutions, the earlier in the processing cycle that data can be converted to a form suitable for machine processing, the greater the economies that can be realized. The rapidity with which EFT services become widely available depends in part on the rate of diffusion of several supporting technologies. Among these are the Touch-Tone® telephone, which allows individuals to send digital messages over EFT networks; home computers and interactive TV cables, which also provide that capability; switching and networking techniques, which facilitate the handling of large numbers of small messages generated between large numbers of comparatively dispersed locations; and improved, more secure access systems. At present, decentralized EFT devices are usually accessed by the combination of a plastic card and a personal identification number, but future systems could use handprints, fingerprints, voiceprints, or signature recognition.

Automated Teller Machines

The EFT technology that appears to have been most readily accepted and welcomed by the general public is the ATM. These provide the banking services used most often by consumers (except for loans). Most transactions can be accomplished faster and more conveniently than with human tellers, and many consumers appear to like the technology. Some use it by preference even when human tellers are available. One big attraction is service 24 hours a day, but customers who rely on this feature are, on occasion, seriously inconvenienced by finding the machine inoperative at a critical moment.

As shown in table 2, ATMs usually allow deposits to and withdrawals from both savings and checking accounts, transfers between these accounts, and queries about the account balance. Some permit the use of credit cards for cash advances. Frequently overdraft privileges are offered with accounts that are accessible through ATMs. Some ATMs have direct access to the financial institution's computer and update accounts immediately. Cash disbursements are limited to either a predefined amount or the actual account balance. Others operate independently of the institution's computer and merely limit the amount that can be withdrawn within a specified period. Actual account balances are updated daily.

ATMs may be located on or off the bank premises; most are accessible around the clock. However, because Federal courts have ruled that an ATM is a branch bank, State laws concerning branch banking limit the possible locations. The debit card used to activate the ATM may be proprietary to the

Table 2.—EFT Services and Technologies

EFT services	EFT technologies			
	POS	ATM	TBP	ACH[a]
Consumer oriented/decentralized services				
A. EFT services that facilitate the transfer of information				
Check authorization	X			
Check verification	X			
Check guarantee	X			
Account status inquiry		X	X	
B. EFT services that involve direct money transfers				
Deposit		X	X	
Cash withdrawal		X		
Bill or loan payment		X	X	
Interaccount transfer		X	X	
Debit of transaction balance with overdraft privileges	X	X	X	
Credit purchase	X			
Cash advance		X		
Institution oriented/centralized services				
Direct deposit of payroll				X
Preauthorized debit services			X	X
Corporate cash management (including interbank and intrabank transfers)				X

NOTES: POS - Point of sale TBP - Telephone bill paying
ATM - Automated teller machine ACH - Automated clearinghouse

[a]Including wire transfer networks.

SOURCE: Office of Technology Assessment and Kent W. Colton, et al., *Electronic Field Transfer Systems and Crime*, Public Systems Evaluation, Inc., February 1981 draft.

bank, offered under the logo of a credit card association, or offered by a third party without showing any financial institution identification. Both the card and a personal identification number are necessary for access. The Electronic Funds Transfer Act of 1978 requires that financial institutions make receipts available to customers at the time a terminal transaction is initiated. The act also requires that ATM transactions be shown on the periodic statement issued by the financial institution.

ATM networks may be proprietary to one institution, or they may be operated on behalf of multiple institutions by consortia or by third party operators. Networks that cross State lines limit services to conform to regulations on interstate banking.

Banks add ATMs to attract new customers and to increase the volume of accounts. In 1981, the cost of an ATM transaction, which is very volume-sensitive, reached a level comparable to the cost incurred using a human teller (1). The estimated average number of transactions per month at an ATM is 5,000, which represents one every 8 minutes around the clock. Some ATMs record as many as 20,000 to 30,000 transactions per month, or one every 1½ to 2 minutes (2). In 1979, the average deposit ranged from $137 in small communities to $248 in large communities, and the average withdrawal from $20 to $37, again depending on location (3). Thus, an average ATM deposit is much larger than an average withdrawal.

ATMs were installed at an average rate of 1,200 per year from 1974 through 1976. By 1979, the number had increased to about 3,000 per year, with a large backlog of orders for 1980 (4). The number of ATMs in operation in 1981 was estimated at 25,000 (5). This should double at least and could rise to 120,000 by 1990 (6). Continuing technological improvement would lower both initial and operating costs and decrease malfunctions and downtime. Changes in banking laws that would permit interstate deployment of full-service ATM networks could enhance their utility, and the availability of interstate access could be cost effective for both users and providers of financial services. Nonfinancial institutions are now offering ATM services through networks that cross State lines. However, interstate deployment by banks can be viewed as the implementation of interstate banking. Some believe that interstate banking could lead to the excessive concentration of power in a relatively few firms in the financial industry, and thus to a situation where financial markets are no longer responsive to local needs.

Point-of-Sale

Point-of-sale (POS) EFT technology deployed in supermarkets, department stores, discount chains, and other commercial facilities offers several kinds of services:

- check validation and credit card authorization,
- direct transfer of funds from a customer's account to the merchant's account by means of a debit card; and/or
- banking services; i.e., direct withdrawal of currency from (or deposit in) a depository account, using the merchant's cash drawer and sales personnel.

POS usually employs a terminal, which may be operated by a store clerk or by the customer, and a telecommunication link to customer information files within the institution providing the service (see table 3). There are an estimated 87,500 POS terminals now in service at retail locations primarily for check validation and credit card authorization (7).

One major problem with POS service is that it establishes a link only between one store (or chain) and one financial institution. It is impractical for merchants to have a terminal for every financial institution. Switching systems are needed, and although the technology is available it is not yet widely used.

Table 3.—Point-of-Sale Services

	Functions and resources at the point of sale			
	Customer operated terminal	Retailer's cash	Store personnel	Bank personnel at retailer's site
Transaction authorization	Customer uses terminal to get authorization before entering the checkout line. Terminal may imprint the check or provide a separate authorization document.	Retailer's cash may be given to the customer once authorization has been obtained.	Check for authorization and dispense cash as appropriate. Accomplish tasks to complete sale.	May operate the authorization and provide documentation to customer.
Fund transfer	Enters PIN or other information required to establish the legitimacy of the transaction.	Probably not involved. May be some cases where the retailer will permit the customer to take change in the form of cash.	Perform the standard tasks required to accomplish a sale.	Not involved.
Banking services	Terminal may be an ATM and is able to handle all aspects of the transaction. Terminal may accept deposits and issue voucher against which the retailer gives customer cash.	Retailer may accept deposits and disburse cash using the register to hold inventory of cash.	May operate a terminal and perform all or some of the functions of a bank teller.	May operate a minibranch in the store, performing all of normal teller functions. Or may provide only limited functions and rely on customers and store personnel to accomplish most of the required tasks between them. In some ways more of a conventional branch than EFT.

SOURCE: Office of Technology Assessment.

Credit Card Authorization and Check Validation

Credit card authorization services are operated by card providers or by organizations that perform processing on their behalf. Clerks use either telephones or terminals to determine whether a card should be honored for a particular transaction. The decision is made on the basis of files that show the total activity of a card. Check validations can be piggybacked onto this service or may be operated independently.

There are two kinds of check validation services—those that have direct access to customer checking account balances (positive files), and those that depend on information gathered from a variety of other sources. These sources include records of a consumer's transactions with the system and data reported by participating institutions, not actual account records. Because these files contain only information that is used to disallow transactions, they are called negative files. Some systems provide only an indication that the transaction is good, while others indemnify the merchant against loss.

Both merchants and customers would benefit from a system that improves check validation and credit card authorization, especially on an interregional or nationwide basis. However, users are wary of any validation/authorization system that may cause embarrassment by unanticipated rejection at the point of sale. Consumer-operated POS terminals, which provide written authorizations that can be presented to a clerk, may be one acceptable solution to this problem.

It is projected that POS-based check guarantee and credit card validation services will be available in 10 to 40 percent of all metropolitan areas by 1985, and that 10 to 50 percent of all transactions within those areas would utilize these services (8).

Debit Cards

Direct transfer of funds from a customer's account to a merchant's account by means of EFT services at the point of sale is less common and the outlook is less certain. Today, debit card transactions are usually processed by the same facilities that process credit card transactions, differing only when the final debit to the customer's account is made. In the future, debit transfers will be accomplished electronically. Consumers would lose some maneuverability in managing their financial resources and scheduling disbursements if the debit card were to replace the credit card. However, the debit card would be convenient as a substitute for cash or a check, for instance, in supermarkets where credit usually is not available. If the cost of credit continues to increase, consumers may regard debit cards more favorably, especially as the use of ATM cards makes the concept more familiar.

The outlook is for financial institutions and joint ventures to take the lead in offering these services. They are likely to be installed first in supermarkets and shopping centers. To be economically feasible, the service requires a shared communication network and improvements in terminals, cards, magnetic tape storage, fiber optics communication, and security (identification) systems. Expectations are that by 1985, 10 to 20 percent of metropolitan areas will have access to these services, and by 1995, as many as 40 percent (9).

Telephone Bill Payment

Many telephone bill payment (TBP) services allow customers to pay bills using a home telephone to instruct a bank computer to transfer money from their account to that of a creditor. Others record the customer's verbal instructions on a tape or through the intervention of a human operator. In the latter case, there is an additional step of transforming the input for computer processing. However, the more widespread availability and use of Touch Tone® service, and the continual increase in the cost of human labor, will lead to the phasing out of TBP services that do not take input directly from the customer. In 1979, 36 percent of residences already had Touch-Tone® telephones. American Telephone & Telegraph projects that this will increase to 64 percent by 1984, and perhaps to 90 percent by 1995 (10). Present Touch-Tone®-based services often use a voice synthesizer to respond to customer inputs. Direct voice input may be available in the future, and at least one device capable of processing voice input for a TBP application has been demonstrated.

A major drawback with TBP service is that the customer has no proof that instructions for payment have been given until a monthly statement is received. This provides the customer's only proof of payment. In case of a dispute, the customer may find it difficult to substantiate claims.

In some systems, a new customer provides a list of those who are to receive payments, and is afterward limited to that list or modifications of it. Signed documents are used as the basis for creating the list of payees and to support any changes that may be made to it. In other systems, the service provider has a standard list of those to whom payments may be made, and all customers are limited to that list. All payments to one receiver are aggregated for some period of time before being deposited to the account. Some merchants have expressed dissatisfaction with TBP since some service providers have not done a good job of coordinating with them.

Thrift institutions were motivated to offer TBP services as a means of getting around the legal prohibition on interest-paying checking accounts. This prohibition was rescinded by the Financial Institutions Deregulatory and Monetary Control Act of 1980. At the end of 1980, there were 302 financial institutions—primarily savings banks—offering TBP, and the Electronic Funds Transfer Association estimates that TBP transactions are now growing at about 27 percent a year (11). The following factors could greatly increase its future use:

- cross-marketing with negotiable order of withdrawal (NOW) accounts;
- continued increases in postal rates;
- increased charges for checking accounts;
- the addition of such services as securities transactions and catalog ordering; and
- development of the capability to encode voice inputs automatically.

The growth of cable television and its use for two-way communication could add a new dimension to TBP services. The popularity of home banking, which concentrates on financial management services such as account transfers, credit applications, and other financial information, is likely to increase as the necessary equipment becomes available in more and more households. Most major banks have plans for testing or implementing these services in 1981-82, and some financial institutions are already involved. However, the ability to either make a deposit or distribute cash via home banking services will be impossible, at least for the foreseeable future (12).

Wire Transfer

This is the earliest form of EFT, since funds have been sent by wire since the first telegraph lines were strung well over a century ago. The transfer of funds by telegraph is chiefly used to move large sums for commercial customers. Financial institutions use Fedwire, operated by the Federal Reserve System, or Bank Wire II, a service provided through a corporation owned by the banking community. Both are now being upgraded to use the newest technology. Commercial banks can connect their computers directly to the wire networks to speed up the process.

The Federal Reserve System is now assessing the question of whether large checks should be presented by wire, with paper checks following only to confirm the transaction. This would help to reduce float and achieve a long-standing goal of the Federal Reserve System.

Check Truncation

Checks conventionally are returned to the writer by the bank and often represent the only receipt for a payment. Checkwriters frequently are careless about filling out stubs, and rely on returned checks for a record of their transactions to support tax returns and for other purposes. But check handling and return are a costly burden for financial institutions, especially with the rising cost of postage.

With EFT, checks can be "truncated" when deposited or at the clearinghouse; i.e., they can be recorded on magnetic tape. Checks may also be retained by the institution holding the account against which they are drawn. The accountholder then gets back only a periodic statement. Since the Bank Security Act requires that all checks over $100 be recorded,* no additional data would have to be recorded by banks other than a check reference number for easy location of the cancelled check. The accountholder, however, has to maintain accurate records so that a copy of a check may be requested in case proof of payment is required. Payee information could be automated and added to the statement if there were public demand for it. However, this would require additional encoding equipment, thus increasing the cost. This information would also be added to the automated information file, which might raise further concerns about privacy.

*Recording of checks under $100 is optional. However, as a matter of routine practice, all checks are recorded.

Automated Clearinghouses

ACHs comprise a centralized EFT system that serves institutions rather than individuals. Instead of having checks sorted and physically dispatched to the debiting bank, an ACH receives, sorts, and distributes payment information on magnetic tape, which instructs banks to debit and credit accounts at a specific time. ACHs are most commonly used by large organizations for direct deposit of payroll "checks" and for collecting preauthorized consumer payments, such as insurance premiums and mortgage payments. Payment transactions initiated by individual consumers using such services as TBP can now be handled through the ACH network. As an alternative to the use of magnetic tape, an ACH can move data directly from computer to computer via telecommunication.

Originally, ACHs handled only batches of transfers, but now individual transfers can be handled one at a time. There are 32 ACHs, 31 of which are operated by the Federal Reserve System. In 1979, they carried 14.5 million transactions in an average month, and transactions were increasing by about 130 percent per year.* Although 60 percent of all financial institutions (about 26,000) participate in an ACH, 75 percent of the traffic is originated by the Government for social security checks, military payrolls, and some civilian payrolls. The U.S. Treasury would like to expand its use of ACH to deliver, for example, all social security checks, all Federal employee payroll checks, and all tax refunds (13). The Treasury estimates that electronic payments cost them only $0.02 each compared with $0.17 for a paper check. Bank costs for handling a Government payment also drop from $0.225 to $0.085. The Federal Reserve System itself suffers a slight penalty; $0.01 for an electronic item compared with $0.005 for a check (14).

*Estimated; Federal Reserve ACH monthly totals, added to New York ACH private volume.

Only a few private companies use automatic payroll deposit, partly because it reduces their float. If postal rates increase sufficiently to offset the benefits of float, and if the Federal Government were to increase its use of ACHs (e.g., requiring Federal employees to accept direct deposit), ACHs should greatly expand in the future. Improvements in minicomputers and data transmission will also encourage expansion. An expanded ACH system could also be used for TBP and check truncation. Within 15 to 20 years, it is possible that virtually all financial institutions and other providers of payment services could be linked in an online, real-time system of exchanges across the Nation through the ACH network (15).

Chapter 2 References

1. "Electronic Banking," *Business Week*, Jan. 18, 1982, p. 76.
2. Linda Fenner Zimmer, "ATM Boom Ahead," *Magazine of Banking Administration*, May 1979, p. 33, and Electronic Banking, Inc. (Sept. 23, 1981 letter from Allen DeCotiis).
3. Ibid., p. 146.
4. Zimmer, op. cit., p. 33.
5. 1981 data from Electronic Banking, Inc. (Sept. 23, 1981 letter from Allen DeCotiis).
6. Based on industry studies and IBM estimates (Sept. 7, 1981 letter from Jerome Svigals).
7. Ibid.
8. Working Paper B., Electronic Banking, Inc., *EFT: The Next 15 Years* (June 30, 1980).
9. Ibid.
10. Ibid.
11. LINK Research Report, *Current Initiatives in Mass Market Transactional Services*, NRR, vol. 2, No. 4, August 1981.
12. Ibid.
13. Information received from Department of the Treasury, Office of Fiscal Assistant Secretary, Operations Planning and Research Staff (August 1979); see also Carl M. Gambs, "Automated Clearinghouses: Current Status and Prospects," *Federal Reserve Bank of Kansas City Economic Review*, May 1978, p. 10.
14. Division of Federal Reserve Bank Operations, Board of Governors of the Federal Reserve System, *Costs, Savings, and Benefits of Electronic Government Payments* (1977), pp. 56; Earl G. Hamilton, "An Update on the Automated Clearinghouse," *Federal Reserve Bulletin*, July 1979, pp. 52-56; Federal Reserve, "The Payment System in the United States," Jan. 25, 1979, pp. 4-7. The $0.005 does not include the cost of "float."
15. Working Paper B, op. cit.

Chapter 3

Competitive and Regulatory Environmemt of Electronic Funds Transfer

BEST AVAILABLE COPY

Chapter 3

Competitive and Regulatory Environment of Electronic Funds Transfer

Chapter Summary

Traditionally, financial institutions have been the providers of payment services. However, market and regulatory forces have encouraged others to enter the market; as a result, the mix of participants in the market is in a state of flux. In response to forces operating in the financial markets, the regulatory environment is also dynamic.

In general, American depository institutions (e.g., commercial banks, savings and loan associations) are no longer merely staid acceptors of deposits and makers of loans. They offer, and sell aggressively, diverse services including electronic funds transfer (EFT) in order to attract new customers, increase the volume of accounts held, and make a profit. In the process, old distinctions between the services offered by banks, thrift institutions, and other financial institutions are breaking down. Moreover, competing services are being marketed by nondepository institutions (e.g., securities brokers, and credit card companies) whose activities are not limited by the regulations that affect depository institutions. Money market funds, for example, allow customers to withdraw funds using "checks" and debit cards.

The key actors in the development of EFT, then, are financial institutions of all kinds; other organizations that offer EFT services; developers and manufacturers of EFT equipment and supporting technologies; telecommunication common carriers; merchants, especially large department store chains, discount chains, and supermarkets; Congress and Federal regulatory agencies; State regulatory agencies and State legislatures; and the public, as consumers and as taxpayers.

The Payments System

There are four ways of making payments—through barter, with cash, with checks, and by EFT. The use of a credit card does not result in a draft on the transaction balance of a consumer. It creates a record of the obligation to pay in the future—almost always by check. However, the use of a credit card *does* effect a transfer of funds to the acceptor from the credit card institution almost immediately upon receipt of a sales draft. Because credit cards are included in much of the debate about EFT, they are included here as an EFT service.

Cash is used in 87 percent of all transactions, but these account for only 3 percent by value (1). The amounts of hard currency exchanged tend to be small—under $10 in 95 percent of cash transactions. This is because cash is still the most convenient method of storing and transferring small amounts of value, and is almost universally accepted. On

the other hand, very large cash transactions involving hundreds or even thousands of dollars sometimes indicate illegal activity and/or attempted tax evasion. Because there is likely to be no audit trail, cash offers a unique degree of anonymity that is not available to users of payment services.

Most "money" in fact exists only as information in the records of financial institutions. To shift funds from one account to another, Americans write about 32 billion checks a year, a number that has been increasing by about 5 percent annually (2). An estimated 81 percent of adults have checking accounts (3). Professionals and managers are most likely to have them, with housewives ranking second at 92 percent. Those who are less affluent and less educated are the least likely to have checking accounts. Nevertheless, over 50 percent of persons in the lower income brackets do maintain checking accounts (4).

Checks are handled an average of three times before they are returned to the writer as a receipt. There are no firm figures on the cost of processing a check. One estimate is $0.15 to $0.20 per check, with $0.50 to $0.75 for "exception processing" of the 2.7 percent of checks that have to be returned to the payee because they are rejected or bounce (5). The total cost of processing checks may be as high as $7 billion annually, excluding the costs to merchants trying to collect for bad checks and the cost of float (6). The desire to reduce the growing burden of check handling and processing is a major incentive in the move to EFT.

Approximately 62 percent of American adults have at least one credit card (7). The average household has 4.5 cards, and there are 475 million cards in use. Department store cards are the most popular, with 66 percent of all households having a card from one of the three large chains—Sears, Ward's, or Penney's. Bank credit cards (such as MasterCard or Visa) are held by 64 percent of households, and gasoline credit cards by 49 percent (8).

Credit cards provide revenue for the service provider in three ways:

1. the merchant takes a discount that goes to the card provider,
2. the cardholder may be charged an annual fee, and
3. the holder pays interest on the debt, usually after a 25-day grace period.

However, financial institutions are prohibited from charging user fees in some jurisdictions, and there are legal limits on the interest that may be charged. Credit cards are not as profitable as they once were; thus, many institutions that provide credit card services would like to switch customers to the use of debit cards, which authorize an immediate transfer of funds from the user's account.

In spite of rising interest rates, as long as the inflation rate remains high, credit cards allow customers to manage their money to their own profit and to extend their financial flexibility. However, since financial institutions now market accounts with overdraft privileges, checks, as well as credit and debit cards, can be used as a tool for money management.

Providers and Regulators of Payment Services

The diverse financial and nonfinancial institutions providing EFT services are subject to different laws and regulatory systems on both Federal and State levels. *Depository institutions* include commercial banks, mutual savings banks, savings and loan organizations, and credit unions. No other institutions can accept deposits. These organizations are chartered either by a State or by the Federal Government, but to operate within a State a federally chartered bank must also have a State license and abide by State laws. EFT services are also offered by *nondepository institutions* including mort-

gage brokers, securities brokers, credit card companies, retail credit organizations, and other loan companies. A variety of specialized services are offered by companies that set up and operate under their own logo, networks of automated teller machines (ATMs) for banks.

Retail finance companies are subject to only limited regulation; brokerage firms are regulated by the Securities and Exchange Commission, but their payment services are almost completely unregulated. Depository institutions are regulated by a number of Federal and State agencies such as the following:

- *The Federal Reserve System (FRS).* All national banks are members. State chartered banks may join. FRS examines and supervises State member banks and bank holding companies. It establishes reserve requirements for members and nonmembers, distributes currency and coin, assists in the processing and clearing of checks for both member and nonmember institutions, and acts as the fiscal agent for the Federal Government. FRS services are paid for by the users.
- *The U.S. Comptroller of the Currency* charters, supervises, and examines national banks.
- *The Federal Credit Union Administration* charters and regulates federally chartered credit unions.
- *The Federal Deposit Insurance Corporation* oversees insured State banks that are not members of FRS, and insures all national banks and State banks that are members of FRS.
- *The Federal Home Loan Bank Board* regulates and insures federally chartered savings and loan organizations and federally chartered mutual savings banks.

In addition, State regulatory agencies oversee the operation of all financial institutions chartered by the State. The so-called "tangled web" of bank regulation is illustrated in figure 1.

Existing and Proposed Laws

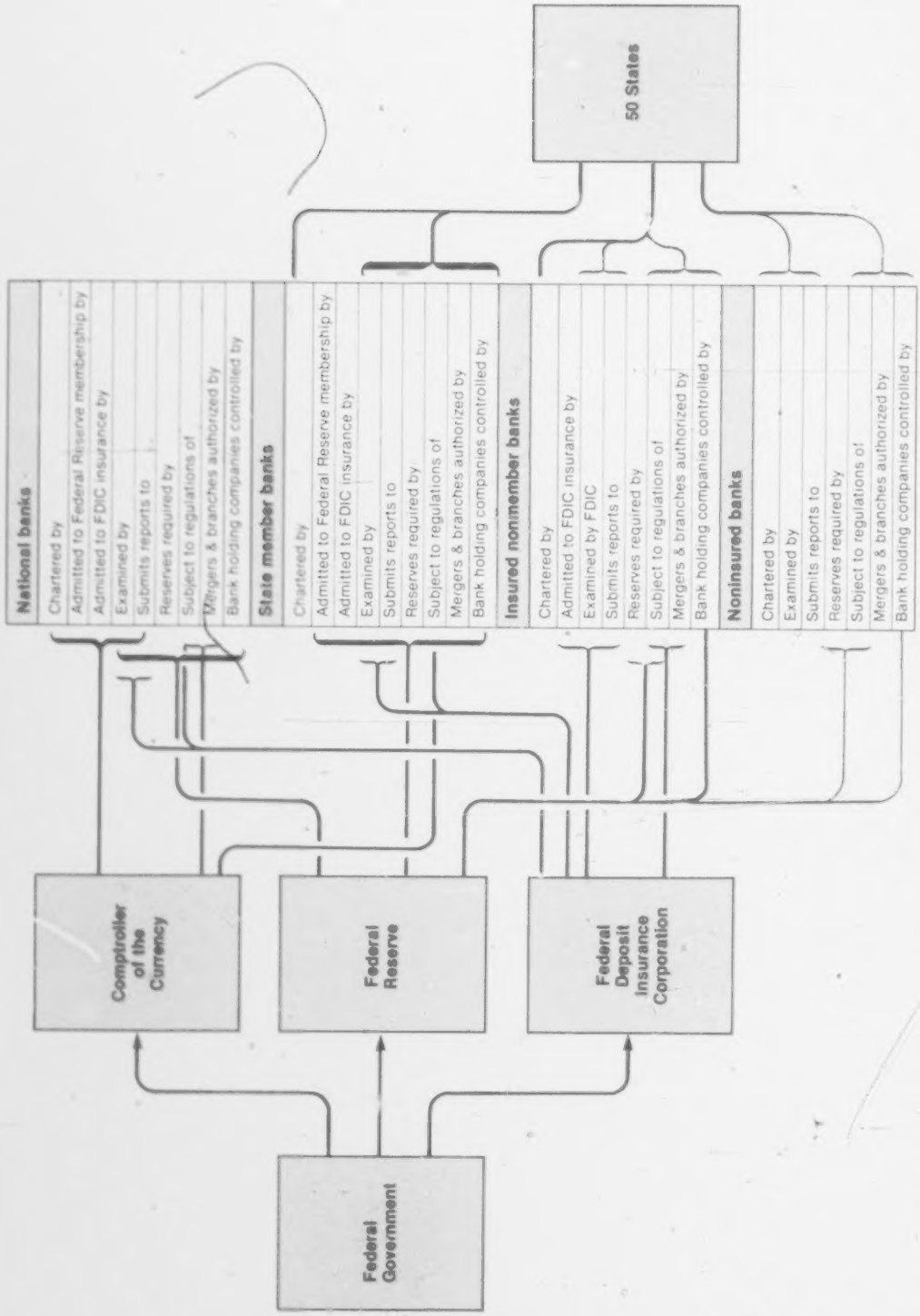
The Electronic Funds Transfer Act is title XX of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (9). This act defines the rights and responsibilities of EFT consumers and providers. For example, the act:

- sets limits on the liability of consumers if there are errors in an EFT transaction or if an improperly authorized transaction is executed;
- establishes the responsibility of consumers for ensuring the security of their EFT accounts and for reviewing statements provided by the financial institutions;
- establishes requirements for the documentation of an EFT transaction that must be provided to the consumer, including definition of the contents of a receipt provided at the time of a transaction and the timing and content of periodic statements that are issued by the service operator;
- establishes rules governing the issuance of EFT access devices.

The Right to Financial Privacy Act of 1978 (10) limits the right of the Federal Government to access financial records of individuals and small partnerships, as well as the right of financial institutions to disclose such records to the Government. It applies only to the Federal Government and not to other organizations and institutions that might seek information.

Legislation that was proposed in the 96th Congress, but not enacted, includes the Privacy of EFT Act (11) and the Fair Financial Information Practices Act (12). The first would protect privacy in EFT systems in

Figure 1.—The Tangled Web of Bank Regulation



SOURCE: *Savings and Time Deposit Banking*, American Institute of Banking, 1968, American Bankers Association.

BEST COPY AVAILABLE

much the same way as letters and telephones are protected; it would provide criminal penalties and would allow victims to sue for damages in civil court when there is disclosure of information to anyone other than participants in the exchange or to Federal agencies with a court order. The Fair Financial Practices Act would establish more specific obligations and rights, such as the necessity to inform consumers of information-gathering practices and policies, and "enforceable expectations of confidentiality." (See ch. 4 for further discussion.)

The 1927 McFadden Act (13) requires that national banks operating within a State abide by the State laws regarding branch banking; it effectively bars interstate branching since State laws generally prohibit such branching. However, foreign-owned banks operating within the United States are permitted to establish branches wherever they can obtain permission from the appropriate regulatory authorities. The McFadden Act prohibits banks from offering some EFT services across State lines, such as accepting deposits through their own ATMs. However, services such as telephone bill payment and the dispensing of cash are offered in some areas without regard to State boundaries. Some smaller banks have expressed the fear that larger institutions will use interstate EFT services as a wedge to penetrate their markets and eventually drive them out of business. As described below, interstate EFT services are now spreading rapidly.

Rules governing EFT services are not uniform among the States. Some prohibit the deployment of terminals because they are considered to be branches, and branching within some States is prohibited. In others, EFT services of all kinds may be offered statewide. Some States require that EFT terminals and facilities be shared among all institutions applying for access; others permit sharing at the discretion of the owner of the facility; some expressly prohibit the sharing of EFT facilities among financial institutions.

The Depository Institutions Deregulation and Monetary Control Act of 1980 (14) has a direct bearing on the legal environment in which EFT will be offered in the future. Specifically, it permits: 1) thrift institutions to offer checking services in conjunction with passbook and share draft accounts, and 2) commercial banks to pay interest on transaction balances.

Thus, some of the distinctions between thrift institutions and commercial banks have been eliminated. Thrift institutions can now offer the full range of EFT services to consumers. At the same time, because they no longer have to use devices such as TBP to get around limitations on the offering of checking services, some of the impetus behind the growth of EFT may have been reduced.

Interstate EFT Services

As already noted, the McFadden Act prohibits interstate banking. But even without direct legislative action, aggressive business decisions are being made and regulatory actions taken which are, in effect, establishing interstate financial services (15). Examples are:

- Rocky Mountain Visa bank cardholders may withdraw cash from their savings or checking (asset) accounts or draw upon a line of credit at ATMs established by participating banks in any of the seven or so States in the region. The interstate withdrawals are based on a legal opinion of counsel that they are the functional equivalent of cashing a check.
- Both Visa and MasterCard had planned to implement national ATM networks during 1981 for cash withdrawals from a

line of credit or asset account. However, this implementation did not take place.
- The cash management accounts offered by nonbanking entities such as Merrill Lynch, Shearson Loeb Rhoades, Dean Witter Reynolds, etc., look, sound, and act like checking accounts, and continue to grow. These nonbanking entities are not presently limited by Federal or State branch banking laws.
- A recent Federal Reserve Board decision concerning the definition of a commercial bank for the purpose of the Bank Holding Company Act will allow bank holding companies to hold chains of "noncommercial" banks across the Nation that may not offer checking accounts, but could provide check-like services such as ATMs or negotiable order of withdrawal (NOW) accounts.
- A ruling by the Comptroller of the Currency that EFT services provided by a bank service corporation do not constitute branch banking by the participating banks—coupled with the Comptroller's earlier ruling that a national bank sharing an ATM established by another entity does not represent interstate branching—provides legal authority for the aggressive development of ATM networks.
- The Federal Home Loan Bank Board has eliminated geographic restrictions on the remote service unit (RSU) operations of federally chartered savings and loan institutions.

This acceleration of the development of interstate services is likely to increase the pressure for revision of banking laws.

Key Actors in EFT Development

The key institutional actors are listed in table 4. Banks and other depository institutions want rapid development of centralized EFT systems to relieve them of the heavy burden of check processing and to reduce their costs. They view decentralized EFT systems as necessary to attract new customers and to increase their volume of accounts in a market that is becoming more and more competitive. Nondepository institutions are seeking ways to compete for some portions of this market, and a variety of nonfinancial institutions strive to make a place for themselves; e.g., by providing and operating EFT devices and networks for the financial institutions.

These participants in EFT development place high priority on continued innovation and technical development to make EFT (especially decentralized systems) more cost effective and more attractive to commercial organizations. Some of the providers believe it is in their interest to respond to concerns about privacy, security, and equity, and to resolve these problems in a way that is fully satisfactory to a concerned public, if only to avoid or reduce the necessity for new legislation and regulations that might inadvertently stifle innovation and continuing improvement in the technology. Other providers believe that privacy, security, and equity are not major problems and therefore do not merit serious attention. At the same time, some financial and related institutions hope for changes in State and Federal laws that will remove barriers to branch banking, as well as other obstacles to interregional and national applications of EFT. Others, particularly the smaller institutions, do not necessarily agree with this view. They have concerns about possible encroachment on their markets by large institutions.

Providers of credit card services (which include retail chains and banks as well as some specialized companies) are finding credit services less profitable than in the past. EFT can help to reduce excessive costs (e.g., by prior authorization), but it also offers the potential for shifting customers from the use of credit cards to debit cards. Providers believe

Table 4.—Key Institutional Actors in EFT Development[a]

Financial institutions

Commercial banks (over 14,000)
: Banks are involved as providers of EFT by offering ATMs and telephone bill payer (TBP) services. Banks also participate in automated clearinghouse (ACH) and point-of-sale (POS) systems, and wire transfers.

Savings and loan associations (S&Ls) (over 4,000)
: S&Ls were in the forefront of EFT development as they tried to use EFT services to gain a competitive advantage on banks. They implemented consumer EFT like ATMs, POS, and TBP.

Mutual savings banks (MSBs) (almost 500)
: Many MSBs were less involved with EFT at the outset since they were pioneering NOW accounts. Today they are involved, like S&Ls, in consumer EFT services.

Credit unions (CUs) (over 24,000)
: Some of the larger CUs were EFT innovators, like S&Ls, and concentrated on EFT consumer services.

Government institutions

Federal Reserve
: The Federal Reserve was instrumental in organizing the first ACH. They have continued to provide leadership in developing standards for ACH and protocols for interregional transfers. They also have a regulatory role.

U.S. Treasury
: The Treasury has provided large transaction volumes to EFT by disbursing Government funds with EFT. Treasury uses direct deposit of Social Security, military retirement, and SSI checks.

Regulators of financial institutions
: Besides the Federal Reserve, there are four other major regulatory bodies: the Comptroller of the Currency, the Federal Deposit Insurance Corporation (FDIC), the Federal Home Loan Bank Board (FHLBB), and the National Credit Union Administration (NCUA). These regulators define the legal environment of EFT for federally chartered institutions. State chartered institutions often come under some Federal control and are also regulated at the State level.

Business institutions

Retail stores
: These stores are involved either by having ATMs on the premises or by installing POS terminals at checkout stands.

Employers
: They participate in EFT by using direct deposit of payroll or by installing ATMs or POSs on premises as an employee benefit.

[a]Does not include the credit card associations or financial conglomerates formed through recent merger activity.

SOURCE: Kent W. Colton, et al., *Electronic Funds Transfer Systems and Crime*, Public Systems Evaluation, Inc., February 1981 draft.

that debit card services can be supplied more efficiently and profitably than credit card services.

In addition to reducing losses from bad checks and credit cards, merchants find that offering EFT services is necessary to safeguard their competitive position. The development of systems that would permit merchants to capture payment and operational data simultaneously, thus helping to control rapidly increasing labor costs, would be most important to them.

The Federal Government's role in EFT is fourfold:

1. provider (e.g., the Federal Reserve System's ACHs);
2. regulator;
3. major customer and user; and, most importantly,
4. ultimate custodian of the public interest.

It is concerned with encouraging innovation and improvement in the technology and associated networks, and with assuring reasonable levels of privacy, security, and equity in its use. State governments share these roles and objectives.

One survey indicates that most Americans are aware of decentralized consumer-oriented EFT services, even though they may not be available in their communities (see table 5). Only a small percentage of people actually use these services now. The most widely available and the most frequently used are preauthorized charges and automatic check approval, but these are often initiated by someone other than the consumer; for example, mortgageholders may encourage the use of preauthorized charges as a payment plan and merchants may refuse to honor checks without validation.

91-217 0 - 82 - 5 : QL 3

Table 5.—EFT Services: Public Awareness, Availability, Usage, and Interest

EFT Services—Awareness, Availability, and Usage

	Awareness	Availability	Usage	Usage index[a]
Automated teller machines	72.5%	31.5%	8.9%	0.283
Preauthorized charges	66.6	42.7	16.6	0.389
Direct deposit of payroll	66.1	36.8	7.5	0.204
Pay-by-telephone bill paying	55.7	17.8	2.5	0.140
Automatic check approval at POS	42.1	24.1	7.6	0.315
Banking at POS	32.0	8.5	1.9	0.224

EFT Services—Interest

	Interest index[b]
Automatic check approval at POS	1.23
Automated teller machines	1.18
Banking at POS	0.63
Pay-by-telephone bill paying	0.62
Direct deposit of payroll	0.60
Preauthorized charges:	
Fixed amount	0.49
Varying amounts	0.31

[a]Computed by dividing the usage rate by the availability rate.
[b]The interest index is computed by dividing the combined favorable attitudinal responses "definitely" and "probably" by the combined unfavorable attitudinal responses "probably not" and "definitely not."

SOURCE: Office of Technology Assessment and *Payments Perspectives '78*, Payments Systems, Inc. and Darden Research Corp.

Chapter 3 References

1. Payment Systems Inc. and Darden Research Corp., *Payment Systems Perspectives '78* (Atlanta: 1978); and Federal Reserve, "The Payment System in the United States" (Jan. 25, 1979), pp. 4-7.
2. Federal Reserve Bank of Atlanta, *A Quantitative Description of the Check Collection System*, 1981.
3. Payment Systems, Inc. and Darden Research Corp., op. cit., p. 53.
4. Ibid., p. 51.
5. Working Paper A, Imperial Computer Services, *Electronic Funds Transfer: The Policy Issues* (May 1979), Part II, "A Typology of Information Relevant to the Study of Electronic Banking," p. 16.
6. Ibid., p. 18.
7. Payment Systems, Inc. and Darden Research Corp., op. cit., pp. 89-90.
8. Ibid., *see also* data from A. J. Wood Research Corp., in *BankCard*, August 1978, p. 2.
9. Public Law 95-630 2002, 92 Stat. 3641, codified in the Consumer Credit Protection Act, 15 U.S.C. 1601 et. seq.
10. Title XI, Public Law 630, 12 U.S.C. sec. 3401 et. seq.
11. S.1929, 96th Cong.
12. S.1928, 96th Cong.
13. 12 U.S.C. 36.
14. Public Law 96-221.
15. Examples from Fred M. Greguras in letter to OTA, Sept. 9, 1981.

Chapter 4

Privacy in Electronic Funds Transfer

BEST AVAILABLE COPY

Chapter 4

Privacy in Electronic Funds Transfer

Chapter Summary

Three principal concerns about electronic funds transfer (EFT) privacy have arisen:

1. the extent to which personal data in EFT systems are or might be disclosed to third parties by financial institutions;
2. the possibility of Government or private surveillance through EFT systems and data files; and
3. the right of consumers to see, challenge, and correct personal data in EFT systems that might be used, for example, to refuse them credit or in other disadvantageous ways.

However, EFT has not yet become a dominant factor in the marketplace, and people have readily available alternatives in carrying out financial transactions. Because of limited market penetration, EFT services so far have led to only minimal consolidations of financial data in any one system.

Some EFT services may not be quite as easy to avoid in the future. Employers may insist on direct deposit of payrolls, social welfare systems may insist on deposit of benefits, and mortgage companies and others may insist on automatically deducted payments. If EFT services become more pervasive, integrated customer files will be more common and public consciousness of the potential for invasion of privacy is likely to increase.

With increased use of EFT there will be a large number of points at which traditional norms of privacy could be invaded. More EFT terminals will be online, making electronic surveillance a more credible possibility. Single-statement reporting of all kinds of financial transactions will become common; more data will be aggregated and thus easier to access. At the same time, there could be broader and swifter dissemination of inaccurate data. Even if customer correction of data is facilitated, it will be more difficult for corrections to catch up with and replace faulty information.

In 1977, both the Privacy Protection Study Commission and the National Commission on Electronic Funds Transfer (NCEFT) recognized that privacy concerns could be especially strong in relation to EFT. NCEFT devoted 19 recommendations to means of protecting privacy.

Only a few of the NCEFT recommendations are reflected in the two EFT-related laws enacted since 1977—the Electronic Funds Transfer Act of 1978 (and Federal Reserve Regulation E) and the Right to Financial Privacy Act of 1978. For example, the use of EFT systems for surveillance purposes is not covered by existing legislation, but would be tightly restricted by the proposed Privacy of EFT bill introduced in the 96th Congress. Disclosure of EFT information to third parties is addressed only minimally by the EFT Act of 1978. However, the proposed privacy of EFT and fair financial information practices bills would provide much more detailed conditions and restrictions on third party disclosure. Even so, these proposed conditions are not as restrictive as some consumers would prefer, and neither one of these proposed bills was enacted in the 96th Congress.

Thus, the needs identified by the NCEFT for more comprehensive EFT privacy protec-

tion, whether through new legislation, modification of existing law, administrative procedures and regulations, industry standards, or some combination, are still largely unmet.

What is Privacy?

It is difficult to define privacy in a precise and concise fashion, even for those who express strong feelings about its value. In terms of information and recordkeeping (as opposed to personal association) it appears to mean, to most people, the ability to keep certain kinds of personal information from other people or to restrict its use, except as one freely chooses to permit its disclosure or use.

In a modern society, it is difficult to keep all personal information absolutely confidential. In practice, individuals generally seek to restrict some kinds of personal information to those who have a legally defined or socially sanctioned need to know, or to those who can provide some benefit or service in return.

There may be many reasons for wishing to withhold information about oneself, other than concern about Government encroachment on civil liberties. Information may expose one to censure or punishment; it may threaten one's reputation, social status, or self-esteem; it may give others some advantage or power over oneself, or lessen one's advantage over others in competitive situations. Information concerning income, debts, or financial transactions may in some situations do all of these things. This may explain in part why people are particularly sensitive to privacy when it comes to payment systems.

Some semantic distinctions may be noted for the sake of clarity. Frequently, privacy is regarded as an attribute of individuals and the focus is on those activities through which they are able to control and restrict access to personal information. The information so protected is "confidential." One way in which privacy can be violated is by illegal or unauthorized access to EFT and other telecommunication systems; the means used to protect the integrity of these systems, and hence the confidentiality of the information entrusted to them, constitute security (see ch. 5). However, the strong possibility remains that EFT systems and services themselves, through their normal functions and operations, may intrude on the privacy of users.

Privacy in Financial Transactions

Only transactions in which currency is the medium of payment can be accomplished with some degree of anonymity. Even then, evidence of financial responsibility often is required in order to obtain a service. For example, it may be virtually impossible to rent a car without presenting a credit card even if payment will be in cash.

When checks are used for payment, a record is created of the payor, the payee, the date, and the amount. In addition, documented identification often is required and various identifying numbers (e.g., telephone number, driver's license, credit card number, employee identification number) may be written on the check by the recipient. The person making payment provides this information willingly in order to have the payment accepted and to enjoy the convenience offered by a checking account. But checks are handled by human tellers and accountants, and the recipient of a check may sign it over to a third party in another transaction.

In order to obtain the further convenience of a credit card, customers are willing to provide additional personal information, such as place of employment, income level, and past financial history. As long as the information is used by the recipient only for the limited purpose for which it was intended, privacy is not usually considered to have been invaded because the information was provided by the subject in order to gain some benefit.

Financial institutions are compelled by law to keep some personal data. The Bank Secrecy Act requires that financial institutions keep copies of all checks over $100 and records of large cash transactions to protect the users of the system. In the same way, the Electronic Funds Transfer Act of 1978, and the Federal Reserve System's Regulation E that implements it, require that receipts issued by EFT terminals and periodic EFT bank statements indicate the date, time, and location from which a transaction was initiated (1).

Personal financial data are not found only within financial institutions and service systems. Employers have records of income, and personnel files may contain other information as well. Tax collectors receive reports of wages, interest and dividends. Social service agencies have records of benefits paid to recipients. Furthermore, people are aware that credit-granting organizations, check and credit authorization services, debt collection agencies, and others collect information about an individual's financial history, both from the individuals and from a variety of other sources not always known to the subject or acknowledged by the collecting organization. People are less aware of the extent to which this information is shared among such organizations or sold to third parties for a variety of purposes, such as compiling mailing lists.

Generally people accept (not always without some irritation and concern) many acknowledged limitations on their privacy, not only because they may have no choice, but because they recognize that they derive substantial benefits thereby. For example, the increased acceptability of one's checks and the ability to obtain credit are benefits that depend on willingness to provide personal and financial information. The aggregation of data about many individuals provides other indirect benefits. Such data are useful for the efficient distribution of goods and services and the management of inventories. Market research may make it possible to design products to meet customer needs and wishes and to identify products that would be rejected in the marketplace, before resources are committed to production. Usually anonymity for individuals can be assured when data are aggregated. However, when data are collected under the expectation that they will be aggregated and then are used on a disaggregated basis (e.g., when survey data become the basis for direct telephone solicitation or lists sold to direct mail advertisers), this may well be considered a violation of privacy, if indeed the individual even becomes aware of the source of the solicitation.

What Constitutes a Violation of Privacy?

In payment systems, privacy is violated when data are, without the subject's consent, made available to and used by those not a party to the transaction, for purposes other than those necessary to accomplish the transaction. Those other purposes could range from organized market campaigns to Government surveillance to blackmail. If a person has neither explicitly nor implicitly consented to disclosure and use of information for a given purpose, personal privacy is considered to have been violated even if the same information was willingly provided by that person, either to another party or to the same party for a different purpose.

There is a second but closely related issue, which for convenience will be discussed under the umbrella of privacy. This is the obverse of unauthorized disclosure of information to third parties; namely, the ability of the individual to know what personal information has been collected and how it is being used. Just as the use of financial data for authorizing the acceptance of payments and the extension of credit is advantageous to the customer, the denial of such services because of erroneous or incomplete data represents a significant disadvantage. Thus, customers need to know what information is recorded about them and how they can correct inaccuracies.

In 1974, Congress passed the Privacy Act (2) to safeguard the privacy of individuals from the misuse of Federal records, to provide individuals access to their records maintained by Federal agencies, and to establish a Privacy Protection Study Commission. In this act the Congress explicitly recognized that:

> . . . the increasing use of computers and sophisticated information technology . . . has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information,
>
> . . . the opportunities of an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems, (and)
>
> . . . the right to privacy is a personal and fundamental right protected by the Constitution of the United States . . .

This act did not deal with EFT systems. However, the Privacy Protection Study Commission was instructed to:

> . . . make a study of the data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the collection of personal information; and
>
> . . . recommend to the President and Congress the extent, if any, to which the requirements and principles of section 552a of title 5, United States Code, should be applied to the information practices of those organizations by legislation, administrative action, or voluntary adoption of such requirements and principles, and report on such other legislative recommendations as it may determine to be necessary to protect the privacy of individuals while meeting the legitimate needs of government and society for information.

The Privacy Protection Study Commission in its 1977 report (3) made several relevant recommendations, most of which have not been implemented. Briefly, they were that:

- data should be used only for purposes for which they are collected;
- subjects should be aware of the uses to which data will be put;
- there should be a proper balance between what an individual is expected to divulge (in connection with financial services) and what that individual seeks in return;
- recordkeeping should be monitored and open to scrutiny by the subject in order to minimize the extent to which information about an individual is a source of unfairness in any decision affecting him/her; and
- obligations with respect to the uses and disclosure that will be made of information about an individual must be established and defined.

EFT and Privacy

In many ways EFT can enhance the privacy of financial transactions. An automated teller machine (ATM) transaction is clearly more impersonal and anonymous than one conducted through a human teller. Electronic transactions cannot be signed over to a third party by the recipient as a check may be. Fewer people are involved in

processing EFT information than in check processing, thus minimizing disclosures due to curiosity or carelessness. The coding of information as electronic signals minimizes the possibility of casual or accidental perusal of information.

EFT includes a number of information-handling services. In some systems the information consists of orders to transfer funds from one account to another; in others the information is somewhat more diverse, and serves as a basis for deciding whether checks should be accepted or credit extended. In each case there is a collector, a conveyor, and a recipient/archiver of the data. The parties or systems filling each of these roles have specific and different needs with regard to the content and form of information, and different potentials for affecting privacy.

The collector obtains information, usually from the customer, and makes an interim record that is retained to provide the beginning of an audit trail to ensure system integrity (see ch. 5). The emphasis is on accurate recording. The data may be used not only to initiate a payment transaction, but also to support internal accounting functions such as inventory control and computation of commissions for salespeople.

Data are passed from the collector to the conveyor or communication link. The conveyor has little, if any, interest in the content of the data; the emphasis is on addressing and routing. However, the message content will be checked to ensure that it has been transmitted accurately. Copies of the data usually are retained for a time to add to the audit trail and ensure system integrity. Copies of data or audit trails sometimes are known as "data puddles;" that is, data that are collected to make the recordkeeping system work and to maintain accurate and secure records. The same controls and protections should be applied to these collateral data as to the records themselves.

Finally, the recipient or archiver receives and processes the data, and implements the transfer of funds or advises on the acceptability of payment or credit. Here the emphasis is on the substantive content of the message.

The collector, conveyor, and recipient/archiver need not be separate. When a retail store uses an electronic cash register connected to a computer to process a charge on the store's own account, it plays all three roles. When a customer uses a bank credit card at the same store, the store acts as the collector, the bank card association operating the communication network is the conveyor, and the bank and/or its processing agent is the recipient/archiver. Each operates under a different set of regulatory constraints that limit the services to be offered and the conditions under which they are offered. The points at which privacy may be at risk are basically the same (collection points, transmission points, and storage points), but the nature and extent of the risk may differ.

In general, there is greater concern about privacy with EFT than with older and more familiar systems for the following reasons:

- EFT makes it easier to collect, organize, store, and access larger amounts of data.
- More data are machine-readable and machine-processable, making them easier to manipulate and aggregate.
- EFT requires less time to record and to extract data; thus it is possible, in principle, to know the physical location of an individual as soon as he/she uses an ATM, or to know details of a transaction as soon as it is completed.
- Some EFT systems use keys such as account numbers, driver's license numbers, or social security numbers that might make it possible to find and integrate many sources of information about the individual.
- Compared to check processing, relatively few people would need to cooperate or conspire in order to violate privacy.
- The number of points at which data are retained may be larger in order to create a useful audit trail.

93-217 O - 82 - 6 : QL 3

- Individual data can be organized and analyzed from multiple perspectives to obtain the maximum amount of intelligence.
- The inner workings of EFT systems are invisible to customers who have no way of knowing what information they contain, who is using it, and for what purposes.

In general, Americans may believe that banks provide more confidentiality for records than is the case. Good data are lacking on the extent to which banks protect the privacy of their customers. In 1979, 130 of the 300 largest commercial banks in the United States were surveyed on this question (4). Since only 34, or 26 percent, of the banks responded, the results are indicative but not conclusive:

- 20% routinely inform customers about the types of records maintained on them.
- 15% inform customers how this information would or could be used.
- 74% do *not* tell customers about routine disclosure of information to Government agencies.
- 85% do *not* inform customers about the possibility of disclosures to private sector entities.
- 88% tell customers the reasons for an adverse decision (e.g., *not* granting a credit line).
- 76% disclose to customers the information behind an adverse decision and its source.
- 36% will let customers see this information.
- 82% tell customers if the bank intends to seek information about them from a third party.
- 30% tell customers the type of information that will be collected.
- 25% tell customers the source(s) that will be used for information.
- 5% tell customers how it will be collected.
- 90% collect some information without telling customers.
- 82% always supplement the information supplied by customers.
- 72% do *not* let customers see the information they collect.
- 100% get information from credit bureaus.
- 34% review the way in which the credit bureau gathered the data.
- 22% use investigative firms to collect information.
- 76% do *not* ask customers before disclosing personal information to third parties.
- 79% have a definite policy about what can be disclosed routinely to Government agents.
- 95% limit the type of information that can be disclosed to nongovernment entities.
- 61% do *not* require a subpoena.
- 58% do *not* have a policy concerning which bank employees have access to customer records.
- 52% allow individuals access to records about themselves, and
  - 86% of these allow the individuals to correct the records,
  - 67% notify other organizations that have received the incorrect data that they have been corrected.

Based on these survey results, it would appear that the protection of privacy at many commercial banks is incomplete and spotty.

The Economics of EFT Privacy

EFT is one of the many technologies growing out of the convergence of computer technology, telecommunication technology, and the technology of information systems. These technologies have greatly reduced the costs of gathering and processing information. The information collected and stored by EFT systems presumably is necessary to the efficient operation of those systems, or is required by law for the protection of customers. Otherwise the costs of collecting and storing it, however small, would not be justified. Some of these costs can be partially offset by selling the data for other purposes, such as commercial mailing lists.

The value of some information depends on its immediacy (e.g., knowing that a credit limit has been exceeded at the moment when a credit card is offered), and some of it has a longer period of value (e.g., names and addresses). However, the value of most information degrades over time except when there is interest in compiling an historical record. The immediacy of access of EFT data adds greatly to their value.

Good information is lacking about the potential costs of enhanced protection of privacy. In 1979, the American Banking Association (ABA) studied 18 representative banks to estimate the potential costs of implementing the recommendations of the Privacy Protection Study Commission (5). The study concluded that costs would be considerably less to banks than to retail lending organizations, since banks already conformed to many of the recommendations as a matter of good business practice. The largest one-time or startup cost would be that of informing customers about institutional policies concerning disclosure and use of customer records. A mass mailing was assumed. However, the study pointed out that this cost could be reduced by including the information in regular periodic mailings to existing customers, and informing new customers at the time the initial relationship was established.

The major recurring costs would be informing customers of the reasons for an adverse decision, providing the information on which the decision was based, and allowing individuals to see and copy this information in order to challenge or correct it. There might also be additional litigation costs, since establishing a statutory right often leads to subsequent litigation. The ABA report indicated that recurring costs could be minimized by routinely informing customers about the basis of an adverse decision in the same letter in which the decision was announced, and honoring their requests "to see and copy" if additional documentation was necessary.

Concern About Government Surveillance

One of the concerns about EFT privacy stems from the fear that an unscrupulous government could use EFT (as well as other telecommunication systems) for surveillance of the population in the interests of political/social control (6). Assuming that there was the will to do so, and that political, legal, cultural, and ethical safeguards against such abuse of government power were weak, scenarios can be constructed in which EFT systems could be used for surveillance. These scenarios would require the following assumptions:

- EFT systems would have to reach a level of use in which they process at least a significant proportion of all payment transactions.
- Organizations providing EFT services would have to be disposed—or forced

—to cooperate in establishing and operating a surveillance system.
- EFT terminals would have to operate in real time.
- It would have to be easier and cheaper —or at least perceived as such—to capture the desired information from EFT systems than in other ways.
- EFT systems would have to be able to capture enough data, in sufficient detail, to meet the requirements of those who seek the information.

Legal Protection of Privacy in EFT

Safeguards for protecting the security of systems are aimed at preventing misuse, destruction, modification, or disclosure of data (as well as theft of funds) as a result of attacks on the integrity of a system; that is, violations of customer privacy that are not initiated or concurred in by the system's designers, owners, manager, or operators (see ch. 5). The concern here, however, is with the possible threat to privacy from the system itself, operating normally; that is, the voluntary disclosure of information to Government agencies or to third parties in the private sector. This kind of protection will be, of necessity, mainly legal.

In 1977, the NCEFT surveyed existing legal safeguards for privacy and made 19 recommendations for further action. Since then, two laws have been passed related to EFT. The Electronic Funds Transfer Act of 1978 and Federal Reserve System Regulation E that implements it make little mention of privacy (7). The Right to Financial Privacy Act of 1978 (8) covers disclosure of records of financial institutions to Federal agencies, but not to State and local governments or to private institutions.

In addition, two bills have been proposed but not passed—the fair financial information practices bill and the privacy of EFT bill. The latter deals with information being transmitted over telecommunication links; i.e., data being passed from collector to recipient/archiver. It covers the records held by a service provider; however, the account records held by the financial institution are not covered.

Because the recommendations of NCEFT covered the outstanding issues regarding privacy and EFT, it is useful to consider how the new and proposed legislation responds to those recommendations.* This is shown in table 6.

Briefly, the two existing pieces of EFT legislation contain little that is directly related to the issue of privacy. What they do contain applies entirely to access to financial records by the Federal Government, which is allowed only under court order for purposes related to law enforcement. However, the EFT Act of 1978 does require that a customer, when establishing an EFT relationship, be fully informed about the financial institution's policies concerning disclosure of information. The act does not require that the customer be informed about specific disclosures or be given an opportunity to contest them.

The proposed fair financial information practices bill would create an "expectation of confidentiality" for information generated by use of EFT systems and services and would allow the customer to sue for damages if this expectation is violated. Disclosures that can take place without violating this expectation of confidentiality are listed. Both of the proposed bills strengthen the existing requirement that customers be fully informed about disclosure policies when subscribing to an EFT service. The proposed privacy of EFT bill also details the conditions under which disclosure of information

*These bills are discussed at length in Working Paper D.

Table 6.—Comparison of NCEFT Recommendations on Privacy With Present Status of Existing and Proposed Legislation

NCEFT Recommendations (Summarized)	Present Status
1. Government should minimize the extent to which it requires an institution to maintain and report records about an individual using an EFT system, and should minimize the extent to which it requires information to be collected that is not necessary to the operation of the EFT system.	Existing legislation, including the two proposed bills, does not deal with this recommendation. The EFT Act of 1978, Sec. 906, specified the data that must be given on EFT receipts and periodic statements and thus could be construed to limit the kinds of data that the Federal Government requires. However, the intent of this section was to provide consumer protection of another kind; namely, protection against error in recording of the transaction and against theft of funds. It is aimed at designating minimum data to be collected. By the same token, however, existing and proposed legislation does not appear to violate the spirit of this recommendation.
2. EFT systems should not be used for surveillance of individuals as to their location or patterns of behavior.	This subject is not dealt with by existing EFT legislation. The proposed Privacy of EFT bill restricts disclosure of information to Federal agencies except under court orders for purposes of law enforcement. According to an analysis by NTIA (Fact Sheet on Privacy in EFT Act) "...the growing use of EFT services, and the potential for surveillance of citizens which that use creates, necessitates effective early steps to ensure that this new tool of commercial intercourse is not misused for private or political prying into citizens' affairs. Whether surveillance is an ongoing interception of an individual's transfers as they occur, or an ex post facto recreation of all of an individual's activities drawn from the records of an EFT service provider, this act effectively restricts disclosure by the service provider while permitting access for law enforcement purposes in appropriate circumstances."
3. Legislation should be enacted to provide that the individual has a property interest in the data maintained by a financial institution about that individual and that Government may get information about depository accounts only with a subpena or administrative summons.	The existing Right to Financial Privacy Act says that an individual can contest such disclosures, but this is not based on a property interest. The fair financial information practices bill creates a clear, legally enforceable "expectation of confidentiality" with regard to non-Federal organizations, but this also does not rest on a property interest. However, the individual is given the right to sue for damages for a violation of the expectation of confidentiality. As it stands, this appears to apply only to violations by a financial institution and not to a nonfinancial institution offering EFT services. The privacy of EFT bill, however, covers disclosure to both Government and private organizations.
4. An individual whose account information is sought by court orders should be given notice before the information is released (except under certain specified conditions).	This recommendation is covered by the Right to Financial Privacy Act of 1978.
5. The individual whose account information is sought under court orders should have a reasonable time to respond and to contest such disclosures.	This recommendation would be met by the Right to Financial Privacy Act of 1978. The customer has 10 to 14 days to respond.
6. Disclosure of information should be made to third parties only: a) if necessary for the operation of the EFT system, or b) for a purpose of which the customer has been informed and to which he/she has consented.	This has not been addressed in existing laws which are both concerned with the relationship between the Federal Government and financial institutions. The EFT Act of 1978, however, requires that when an account is opened the customer must be told "under what circumstances the financial institution will in the ordinary course of business disclose information to third persons." But there is no guarantee that customers will be told about specific disclosures when they occur or that they can then contest them. The proposed fair financial information practices bill has language about preservice notice and gives very detailed conditions under which information may be disclosed. Summarized, it provides for disclosure: • when permission is given by the subject individual. • when required by a Federal or State statute or regulation. • to Government, to defend the financial institution against fraud, when there is evidence of illegal activities related to the account in question, or when the Government requests such disclosure under existing laws. • to litigants, under provisions of the act.

Table 6.—Comparison of NCEFT Recommendations on Privacy With Present Status of Existing and Proposed Legislation—Continued

NCEFT Recommendations (Summarized)	Present Status
6. Continued—	• for purposes of marketing, if the customer has been offered and has refused an opportunity to object to the disclosure and if the information is disclosed by the third party recipient only to the subject. • to someone who is performing business or legal services for the financial institution, such as auditing. • to another depository institution, consumer reporting agency, or authorizing service. • to self-regulating organizations. • to the customer who is the subject of the file. The customer must be fully informed about these conditions for disclosure when the EFT relationship is established. The proposed privacy of EFT bill sets similar conditions for disclosure: • to a Government authority, pursuant to other laws. • to an officer of a financial institution, only to determine if a transaction was correctly carried out. • with specific authorization by one of the participants to a transaction. • when the data are not identified with a particular individual. • if criminal activity is indicated.
7. There should be no disclosure to private sector third parties without specific authorization by the subject, and certification by the recipient that data will be used only for the designated purpose.	This is not covered by existing legislation, but see comments under *recommendation 6*, above, concerning the proposed fair financial information practices bill.
8. Information may be given to support organizations performing routine services for the financial institution, provided it certifies that it will maintain confidentiality.	This is not covered by existing legislation, but is covered by the proposed privacy in EFT bill, except that certification is not specifically mentioned.
9. Information may be disclosed to participants and intermediaries to a transaction; "intermediaries" include authorizing/guaranteeing services.	This is not covered by existing legislation, but is covered by the proposed fair financial information practices bill. See comments under *recommendation 6*, above.
10. Information necessary to ensure the existence or good standing of an account may be given to credit bureaus and authorizing/guaranteeing organizations.	This is not covered by existing legislation, but is covered by the proposed bills. See comments under *recommendation 6*, above.
11. The credit part of an account (i.e., a line of credit or automatic draft privileges attached to an account) may be disclosed to other credit-granting or credit-authorizing organizations and other EFT organizations.	This is not specifically covered by either existing legislation or proposed legislation.
12. Information related to fraud and other crime can be disclosed to law enforcement officers, and customer delinquency or fraud can be disclosed to other EFT-offering institutions, credit-granting organizations, etc.	The first part of this recommendation is now covered by the Right to Financial Privacy Act of 1978, as well as by both proposed bills. The second part is not explicitly covered by either existing or proposed legislation.
13. Names and addresses may be provided for direct mail solicitation unless the customer objects. The customer should be sent written notice that this may occur and be provided a simple means of objecting.	This is not covered in existing legislation, but would be covered by the proposed fair financial information practices bill.
14. Disclosure to any third party is permissible with express written consent from the subject.	This is not covered by existing legislation. Both of the proposed bills cover it.
15. When establishing an EFT relationship the customer should be provided with full information about these policies.	This is fully covered by the existing EFT Act and Regulation E, and is also covered in the proposed fair financial information practices bill.

Table 6.—Comparison of NCEFT Recommendations on Privacy With Present Status of Existing and Proposed Legislation—Continued

NCEFT Recommendations (Summarized)	Present Status
16. Customers should have access to all recorded information about them and be able to correct it.	This is not covered explicitly by existing or proposed legislation. The NTIA commentary on the proposed fair financial information practices bill nevertheless says: "Current law and practice already provide these aspects of information privacy protection in what appears to be an effective and workable manner. Provisions regarding customer disputes and correction of account information already exist under the Uniform Commercial Code and various State laws (for depository institutions). . . (Customers are given additional access rights in other parts of the fair financial information practices bill, in title I, II, III, and V, regarding consumer reporting agencies, credit grants, check and credit authorization services, and insurance companies.")
17. Specifically, the Fair Credit Reporting Act should be amended to provide that: a) organizations that provide authorization/guarantee services are subject to the provisions that apply to credit reporting agencies, except for the requirement that the organization notify prior recipients of information that is later disputed and found to be of questionable accuracy. b) Institutions that decline to honor a check, debit, or credit presented by an individual because of a report by an authorization/guarantee service should provide the customer with the name and address of the service . . . c) The individual has the right to inspect, copy, and have interpreted these records subject to certain conditions.	This is not covered by either existing or proposed legislation. See comment under *recommendation 16*, above.
18. NCEFT used this recommendation to concur in two recommendations of the Privacy Protection Study Commission, saying that EFT services should retain records only for a limited time, and should provide ways for the customer to correct records generated by EFT services. NCEFT disagreed with the Privacy Protection Study Commission recommendation that no Government entity own, operate, or manage any EFT system handling transactions among private parties (e.g., Federal Reserve's ACHs).	This is covered in the discussion concerning *recommendations 6, 16,* and *17.*
19. The Federal Reserve should follow rules at least as confidential as those of private sector EFT operators, and access by other Government agencies to ACH should be as restricted as access to other financial institution records.	As private sector EFT privacy practices are currently mandated by law in only a rudimentary fashion, this recommendation is not fully applicable. According to the Federal Reserve, their policies are consistent with this recommendation. Records of transactions are held for a minimum period of time, and there are long-standing restrictive policies about granting access to information.

SOURCE: Office of Technology Assessment.

does not violate the expectation of confidentiality. These conditions are not as restrictive as some customers would prefer; for example, a financial institution may provide certain kinds of information about customers not only to check-authorizing services, but also to credit-offering institutions (e.g., retail stores, credit card services, etc.) and other EFT systems; and may provide names and addresses of customers to direct mail advertisers and marketers unless the customer explicitly objects in writing.

Neither existing nor proposed legislation directly provides guarantees that customers may inspect, contest, and correct their records held by all EFT offerors. While the National Telecommunications and Information Administration argues that such rights are provided by other (non-EFT) legislation, it is not entirely clear that such is the case (9). The burden of proof with regard to the accuracy of records has not been clearly established through legislation. U.S. privacy laws (both existing and proposed) rely largely on the protesting citizen as the primary initiating and enforcement agent. Yet this assumes that financial institutions have diligently informed the customers about the content and use of their records. As the 1979 survey of banks shows, this assumption of good faith is not necessarily justified. New approaches to privacy protection may be needed (10).

Chapter 4 References

1. Title XX, Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-360, 2001, 92 Stat. 3641, codified in Consumer Credit Protection Act, 15 U.S.C. 1601.
2. 88 Stat. 1896; 5 U.S.C. 552a note; Public Law 93-579, Dec. 31, 1974. The first quotation is from the preamble.
3. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977).
4. David Linowes, *A Research Study of Privacy and Banking* (University of Illinois, 1979).
5. Touche Ross & Co., *Privacy Protection Cost Study* (1979).
6. For example, the Sentry Life Insurance Company conducted a study entitled "The Dimensions of Privacy" (1979) which indicated that 48 percent of Americans are worried about how the Federal Government will use personal information it gathers. *See also* Working Paper D: The Irvine Research Corp., *An Assessment of Equity and Privacy Issues in Electronic Funds Transfer Systems* (September 1980), pp. 100-105.
7. The Electronic Fund Transfer Act (EFTA) and Regulation E merely require that a financial institution's policies concerning the circumstances "in the ordinary course of business" under which it will release information about the consumer's account to third parties be disclosed to the consumer. Some practical implications for personal privacy have, nevertheless, resulted from this law.

   Reg. E's model disclosure clauses suggest that the "ordinary course of business" at the very least means: 1) when it is necessary to complete a transfer, 2) in order to verify the existence and condition of the consumer's account such as for a credit bureau or merchant, 3) in order to comply with governmental agency or court orders, or 4) with the consumer's consent. Many financial institutions have routinely copied the model clauses into their disclosures, thereby creating a contractual obligation to the consumer to handle information in the manner prescribed "in the ordinary course of business." A consumer could also bring a suit under the EFTA if the financial institution violates the law's disclosure requirement. This is considered by some experts to be an important protection of personal privacy. (Sept. 9, 1981, letter to OTA from Fred M. Greguras, Kutak, Rock & Huie.)
8. Title XI, Public Law 630, 12 U.S.C. Sec. 3401 et. seq. *See* Working Paper D, App. D, p. 4.
9. Robert C. Zimmer and Theresa A. Einhorn, *The Law of Electronic Funds Transfer* (Washington, D.C.: Card Services, Inc., 1978), pp. 23-31 ff.
10. Donald A. Marchand, "Privacy, Confidentiality and Computers: National and International Implications of U.S. Information Policy," *Telecommunications Policy*, September 1979.

    Also, the recent adoption of the Organization for Economic Cooperation and Development (OECD) guidelines for personal privacy could be an important factor in future congressional policy determinations. In September 1980, the OECD, to which the United States belongs, adopted guidelines that recommend basic principles of fair information practices and urge nations to remove or avoid creating obstacles to international data flow in the name of privacy protection.

    Under the guidelines, OECD members may restrict data flows to countries that do not substantially observe the fair information

practices principles. Because the United States does not have privacy laws corresponding to those of many OECD nations, especially European countries, the U.S. Department of Commerce is recommending voluntary compliance as the best means of avoiding restrictions on international data flows. One possible consequence of not adopting the guidelines is that other nations could limit the flow of personal and commercial data communications with the United States, which in turn could be a primary impetus to enacting more comprehensive privacy legislation in this country. (Sept. 9, 1981, letter to OTA from Fred M. Greguras.)

Chapter 5

Security in Electronic Funds Transfer

BEST AVAILABLE COPY

Chapter 5

Security in Electronic Funds Transfer

Chapter Summary

Security means the protection of the integrity of electronic funds transfer (EFT) systems and their information from illegal or unauthorized access and use. Although the loss per theft appears to be greater than for paper-based payment systems, there is no real evidence that EFT systems to date have resulted in a higher than average crime rate. Why, then, is the security of EFT systems an important public concern and potentially a major policy issue? In comparison with other payment systems, EFT appears to have some additional vulnerabilities:

- EFT systems have many points of access where transactions can be affected in unauthorized ways because of direct customer involvement with the dynamics of the systems, the use of telecommunication lines, and the ways in which data are aggregated and transmitted among and between sites and institutions.
- Funds can be removed in currency almost instantly without review of individual transactions by officials.
- Because of the kinds of information recorded and the way it is aggregated, EFT data have an economic value above and beyond the value of the funds, and hence provide another source of temptation.
- It is possible, in theory, for large banks of data to be destroyed by remote agents, creating the opportunity for maliciousness, extortion, blackmail, or terrorism.
- EFT crime provides a sporting element, or intellectual challenge, to some people that is perhaps as enticing as the opportunity for financial gain.
- EFT crime is often difficult to detect because funds/data can be removed or manipulated by instructions hidden in complex computer software; the dynamics of the criminal action may be understood only by a few experts within the institution.
- EFT crime is poorly reported because publicity may draw attention to ways of attacking the integrity of the EFT system, may give organizations a poor public image, or may even raise insurance premiums.
- Existing legislation may not be fully adequate or appropriate for prosecuting EFT crimes.

A high degree of security is especially important to the future development and use of EFT because this is a relatively new technology that is challenging much older and well-established payment systems. Therefore, it is particularly dependent on the confidence of the public. The failure to gain and maintain the confidence of individual and organizational users during this period of rapid development could ultimately undermine the stability of financial institutions that have already heavily committed themselves to EFT systems and practices.

It is difficult at present to assess the level of EFT security violations because there is underreporting of EFT crime, a paucity of information about EFT security, and a lack of informed public discussion, although considerable public concern is voiced. Such evidence as is available suggests that EFT security violation is not a severe problem, although the magnitude of loss in individual EFT thefts may be much higher than that in

conventional thefts from financial institutions. While there are some dangers that giving these problems higher visibility through public discussion may at first make them worse, the public is entitled to know what risks they are exposed to in using EFT services. Furthermore, both law enforcement agents and financial institutions would benefit by sharing information about vulnerabilities, defense strategies, and security-enhancing technologies.

Some believe that both effective technology and sound management procedures exist for adequately assuring EFT security, though even present technology and procedures are not all widely used. There is as yet no clear and consistent set of industrywide security standards for protection of computer systems. The use of security technology and procedures varies among institutions. The cost of providing a reasonable degree of security—equal at least to that provided for paper-based payment systems—is probably not excessively high, but information on this point is scanty.

Better information about EFT security would allow Congress and State legislatures to assess more effectively the possible need for new or modified legislation and/or regulations.

Security in Payment Systems

An important issue with regard to EFT is the level of security that will be required and its cost. Will new legislation be needed for prosecution of EFT-related crime? Will public discussion of EFT security problems exacerbate those problems, and if so, is some mechanism needed for sharing information about security problems and appropriate defense strategies?

Any payment system and any financial institution must be able to guarantee, at least to some reasonable degree, the safety of assets entrusted to it. It must be able to protect both funds and data against theft, loss, and misuse. Users must be assured that transactions will be carried out according to their instructions. The ability to guarantee the integrity of the payment system and the safety of both funds and information is what is meant by security.

Any medium of exchange, whether currency, checks, bills of credit, or recorded electronic signals, ultimately relies on public confidence that it will retain its value and continue to be acceptable to others in exchange for goods and services. Similarly, the continued viability of financial institutions depends on the confidence of their customers. Thus, the adequacy of EFT security systems is important, not only because individuals are entitled to protection of their accounts and to the confidentiality of the information that they provide, but also because an unacceptable number of security failures could undermine public confidence in financial institutions, thus weakening the national economy and ultimately the national security.

Wherever monetary value exists, and in whatever form, it becomes an object of greed and a target for criminal activity. Funds have been embezzled and banks robbed for as long as banks have existed. EFT offers some valuable opportunities for protecting individuals and organizations against loss of assets. The availability of automated teller machines (ATMs) and point-of-sale (POS) terminals enables individuals to carry less cash on their persons. Automatic deposit of payrolls and social security checks would reduce the volume of thefts from mailboxes. Merchants will suffer fewer losses from bad checks and credit card fraud. Financial institutions can reduce employee error, improve audit trails, and reduce overdrafts.

However, EFT also has some vulnerabilities that paper-based payment systems do not have, and it creates the opportunity for

new kinds of white-collar crime (1). Most funds have always existed only as data in account ledgers or files. Before EFT, however, the customer was kept at a distance from all but the first and last steps of transactions, and financial institutions could control and guard most of the processing so that risks were at least limited to those internal to the financial institution (with the exception of bank robbers and check passers). Some time had to elapse before funds could actually be removed in the form of currency and could no longer be returned simply by reversing the paper transaction.

With some EFT procedures, however, customer involvement with the system is facilitated and funds are quickly removed, often without another human having overseen the process. Other EFT systems involve many third parties in encoding, transmitting, or storing data, thus providing many vulnerable points where security could be breached. Communication links are vulnerable to electronic eavesdropping and provide entry into the system at several points. The data needed for EFT systems are easily aggregated and accessed, thus creating a value apart from and in addition to the value of the funds. This also creates concern over security in relation to EFT systems.

Security also may be breached accidentally. EFT technologies can lose data through failure of hardware components or communication links, or deterioration of storage media. Where there is no backup documentation such data loss can seriously compromise the system.

Another difference between EFT and traditional security risks related to banking and payment systems is the sporting element. Armed bank robbers are almost always professional criminals. Embezzlers, while they may never before have committed a crime, are motivated just as clearly by greed for financial gain. But it appears that computer criminals are sometimes motivated, at least initially, by the sheer fun of beating the system. This kind of gamesmanship, for a lark as much as for funds, seems to provide the motivation for bright college students and even younger children breaking into institutional computers to discover, modify, or steal information or merely to play tricks on the system.

In the case of EFT systems, however, the sporting behavior is apt to be lavishly rewarded and the fun amplified by substantial financial gains at minimum risk. Some experts assert that most EFT crime is never detected, or if detected is not reported.

Financial institutions are reluctant to publicize EFT losses for several reasons. They fear that public confidence will be compromised and the institution weakened; that their insurance premiums will be increased; and that other computer buffs, or more professional criminals, will learn the system's vulnerabilities or will be challenged to surpass the achievement.

Losses from individual accounts may go undetected by the account owners because they are so small; one strategy is to instruct the computer to deduct a cent or two from each transaction handled, and deposit it in a fraudulent account. A sufficiently high volume of transactions could make such amounts accumulate rapidly. Since information, unlike money, can be owned and used by many people at the same time, data can be "stolen" without anyone being the wiser. By the time stolen information is actually used for unauthorized purposes it may be impossible to trace its origin. Often managers and law enforcement officials are not qualified to detect computer-based crimes and frauds, and are unlikely to challenge either the machine or the computer experts on the workings of the system.

Typical computer criminals are said to be young, intelligent, enthusiastic computer buffs with no prior criminal record and probably no previous criminal activity (2). If detected, they may be either hired or maintained as employees by the financial institution they victimized to help protect it against similar violators. In any case, they

are unlikely to be severely punished. One estimate is that only about 3 percent of computer criminals who are apprehended ever go to jail (3).

Many States do not have legislation for prosecuting computer-based crimes, and even Federal law is unclear in some aspects. In one case, a Federal judge ruled that movement of a stolen program over telephone wires did not legally constitute theft of trade secrets, since the relevant statute required the stolen article to be tangible (4). The act of copying the program and taking it to the thief's office, however, was judged to be criminal. Legislation proposed in 1979 but not enacted, known as the Federal Computer Systems Protection Act, was designed to facilitate prosecution of offenders charged with computer-based crimes against Federal systems (5).

Types of EFT Crime or Breaches of Security

Breaches of security can be accidental as well as deliberate. They may affect individual accounts or threaten institutions or networks. EFT crimes may be aimed at theft of funds; at use, disclosure, alteration, theft, or destruction of data; or at disruption or destruction of the EFT system. Funds (or data) can be stolen by embezzlement within the financial institution, by intruders from outside of the institution, or by customer fraud.

Employees of the institution are frequently the source of EFT crime. They are likely to have access to the systems and often can mask criminal actions behind legitimate activities. They may hide unauthorized procedures within programs (the "Trojan horse" strategy) by building in instructions to abort or divert authorized transactions, and then remove this procedure from the computer's memory bank. Unauthorized copying of either programs or data, such as account numbers and personal identification numbers (PINs), usually cannot be detected or traced (6). However, most reported cases of EFT crime are not sophisticated.

Most of these criminal tactics can also be used by intruders from outside of the EFT payments systems (7). For example, in the hands of a computer expert, a home terminal can successfully "impersonate" a POS terminal and send perverse instructions over the EFT communication line. However, this is difficult to do at present.

EFT communication links can be tapped or used for eavesdropping under some circumstances. False information can be entered or legitimate information altered or destroyed. The lines themselves are also vulnerable.

Customers often abuse EFT systems by unauthorized overdrafts. Some ATM devices are not online; that is, they do not have access to customer accounts. Instead they limit the amount of money that may be withdrawn by a customer with proper identification (usually $100 per 24 hours). Some offline ATM devices cannot lock out stolen cards. Most ATMs, of course, require both an authorized card and a PIN for access. However, some require only a card, and users often carelessly discard receipts bearing their account number right at the site. Against all advice, some users insist on writing their PIN on the access card or on something that they keep with the card.

Access cards can also be forged. They may be stolen from the bank or from the mail enroute to the customer. (Sometimes they are sent to potential customers without having been requested, although an additional validation step is usually required before they can be used.) Account numbers and PINs can be lifted from the card's magnetic strip and transferred to blank cards (8).

ATMs and POS terminals were not in use during the height of political activism and

protest demonstrations of the late 1960's and early 1970's. With any new wave of protest, however, they would be vulnerable to politically inspired vandalism. Spray paint, gum, glue, or objectionable substances would easily render a machine inoperable, at least temporarily.

Normal failures of EFT components or communication links also make EFT devices temporarily inoperable. ATMs currently have an outage rate of about 3 percent (9), which is frustrating to customers who depend on the machines to complete transactions outside of normal banking hours. As more and more customers come to depend on EFT, downtime will be even more unacceptable. Failure of system components can also cause loss of data, which is a more serious matter.

The vulnerability of EFT systems to natural disasters such as earthquakes, floods, fire, and severe ice and snow storms is a matter of some concern. As yet, however, there has been only one reported incident of EFT systems being affected by natural disasters. When Mount St. Helens erupted, many ATMs were disabled by dust and ashes from the volcano. A number of banks have reported that ATMs generally continued to function well during severe winter weather, even though user demands were much heavier than at other times (10). It has recently been suggested that electromagnetic pulses, such as might result from nuclear weapons use, could knock out systems over a very wide area (11). As EFT networks are built, such vulnerabilities become systemic rather than localized. (The larger issue of national security and systems vulnerability is discussed briefly in app. A.)

How Serious is EFT Crime at Present?

No one knows for certain how serious the problem of EFT theft really is, since much of it is either not detected or not reported. Clearly the potential for crime is great. In general, it is thought that EFT thefts aimed at institutions tend to be much larger than traditional forms of bank robbery. One expert estimates that the average armed bank robbery in the mid-1970's netted about $10,000 and the average conventional embezzlement about $20,000, but computer-based banking thefts averaged about $500,000. However, these figures are based on 46 cases of computer-based theft examined 5 years ago when EFT was much less widespread (12). A successful and undetected EFT thief could attack an institution repeatedly, and an institution with an unsuspected vulnerability could be victimized by multiple criminals.

The extent of petty theft from ATMs is also not known. A 1978 survey of financial institutions by the American Bankers Association reported that only 5 percent of the responding institutions were willing to say that ATM losses were greater than those experienced with paper-based transactions, 9 percent reported no losses, and 43 percent reported minor security problems. Of the losses reported, 65 percent by dollar volume resulted from stolen access cards, 22 percent from customer fraud, and 13 percent from "internal problems" (13). Customer fraud usually involved overdrafts at offline ATMs. Reliability failures of the machines (e.g., failing to print a record of disbursements) accounted for some losses. In 1979, the Federal Reserve System reported that ATM losses reported by 125 banks amounted to less than 1 percent of dollar volume of transactions and less than $0.03 per transaction (14). A survey by Payment Systems, Inc., estimated average annual losses at about $0.03 per active card (15).

Another survey reported that customers have been robbed while using ATMs at 2.5

percent of reporting institutions (16). All of these surveys are based on reporting by financial institutions (and only those institutions that responded to questions). They probably understate the facts, but there is no real evidence that EFT systems have resulted in greater losses by theft, fraud, or system failure than result from other payment systems. While EFT creates some vulnerabilities that are not associated with other payment systems, it also offers some advantages in terms of security. For example, it could reduce the number of thefts of checks from mailboxes. Thus, while wide implementation of EFT systems will almost certainly result in shifts in the types of crime associated with payment systems, the degree to which it might result in an increase in the number of crimes, or the dollar volume of losses, is unclear at present.

What is clear is that much of the risk to payment system security can be avoided or reduced with increased attention to protective procedures and security technology.

Technology and Techniques for Increased EFT Security

The major categories of threats to EFT security are summarized in table 7. In theory, nearly all of these can be minimized by the application of good management practices. The three lines of defense against breaches of EFT security are administrative procedures, physical protection, and technical/electronic safeguards.

Personnel within financial institutions or associated with handling, transmitting, and storing data are probably the most important source of risk to security. Good management requires strictly limiting access to funds and data, and keeping full records of who has access and at what times. Personnel must, of course, be carefully selected and judiciously supervised. They can be rotated in their jobs to limit the time they have to experiment with EFT systems and probe for vulnerabilities. It may be possible to divide critical data, such as a transmission encryption key, between two or more people. In some cases, it is possible to divide processing duties so that few people know all of the procedures and programs. However, this is often difficult since EFT by its nature integrates the flow of processing. Audit trails can be established and transaction logs carefully isolated and physically protected. Account activity can be reviewed regularly to detect unusual increases in frequency or size of withdrawals or account balances.

ATMs can be protected by judicious siting—well-lit, heavily traveled locations, usually under public observation—and, if necessary, by armoring. Online ATMs (those with access to customer files to check account balances) prevent unauthorized overdrafts. Both ATMs and POS terminals can be designed so that the user's hands and the keyboard are hidden from observers. In the future, the combination of access cards and PINs may give way to or be augmented by safer access systems using recognition of fingerprints or hand geometry, signature dynamics, or even voiceprints. Technology that allows reliable authentication of human and machine "signatures" is already available (17).

These protective measures have some potential drawbacks. They increase the possibility of unjustified rejections that cause inconvenience, embarrassment, and frustration for the user. They remove the option of sending an agent to carry out a transaction, and at best may cause the devices to appear more "unfriendly" to customers who already are inclined to object to their impersonality.

Table 7.—Major Categories of Threats to EFT Security

Internal threats (within the institution)
System failure:
Failure of computer programs
Failure of hardware components
Loss of data from system malfunction
Deterioration of storage media
Failure of communication links
Failure of power, destruction of facilities
Deterioration of storage media
Employees:
greed, malice, ineptitude, accidents, disgruntlement, challenge
Trojan horse (unauthorized procedures hidden within programs)
Bogus transactions
Unauthorized copying of data or programs
Modification of data
Unauthorized sale of data
Destruction
External threats to system
Natural disaster: fire, flood, ice and snow, earthquake, etc.:
Direct damage
Lack of maintenance
Overload at terminals
Inaccessability
Human:
criminals, terrorists, political (and religious, economic, racial) activists, "buffs," inept customers
Physical damage (including vandalism) or destruction
Destruction of data
Modification of data
Theft of data
Fake transactions
Impersonation of computer
Forged access devices
Unauthorized use of access devices

SOURCE: Office of Technology Assessment

Measures are available to reduce the likelihood of access cards being forged. For example, they can be made sensitive to heat and pressure which are used in illegal duplicating of the magnetic strips. The French and others are experimenting with "intelligent cards" that use a microprocessor to provide access data (18). PINs are almost always transmitted to the customer separately, with instructions that they are not to be written on or attached to access cards. Sealed mailers are frequently used, with the PIN printed through the envelope so that it is never exposed to view even while still within the provider institution. Rather than being assigned a PIN, customers may be permitted to select their own. Technologies are available that prevent the exposure of a selected PIN, even to the system operators.

Institutional computers are generally enclosed and guarded; access is limited and sign-in procedures are used to record entry. They can be protected with monitoring devices and alarms to guard against fire, flood, and intruders. All equipment can be designed to require keys for access and operation. More sophisticated protective procedures include protocols to guard against unauthorized insertion of data or instructions, and procedures that record every modification and every use of programs. Communication lines can be protected with alarms against taps, and tested frequently for eavesdropping.

The best protection for data in transmission and in storage is probably encryption. One form uses encoding in which the coding and decoding procedures are public but the actual encryption keys used are secret and tightly controlled. The National Bureau of Standards has developed a national encryption standard called the Digital Encryption Standard (DES). Another technique never permits the data to exist as clear text that can be understood by humans. While encryption cannot be absolutely safe (every code can in theory be broken with the use of computers), procedures can be used that would take so long to unravel that it would never be worth the effort. For example, some experts suggest that it would take hundreds of millions of dollars and hundreds of years to crack DES (19). Another important but expensive security measure is the provision of backup for computer processing, data storage, communication lines, and power sources.

While technology both to provide and to breach security will undoubtedly continue to develop in parallel, it seems clear that the application of good management procedures —combined with physical protection, backup facilities, and electronic technology—can

provide a substantial level of security, but at considerable cost. The issue, then, concerns the appropriate balance between cost and additional security.

Security and Public Discussion

The customer is often directly culpable in violations of security, quite apart from intentional customer fraud. EFT users often ignore all warnings and handle access cards, credit cards, PINs, and account numbers with great carelessness. They write PINs on ATM access cards, discard receipts beside ATMs, fail to report the loss or theft of cards, and leave bank statements lying around. Public education about EFT security risks and vulnerabilities therefore would seem desirable.

However, financial institutions are reluctant to call attention to these problems or to encourage public discussion of security issues. This is not entirely because the competitive position of their own services may suffer, or even because it might contribute to loss of public confidence in EFT. They are understandably reluctant to promote the realization that EFT offers a new and potentially lucrative field of crime, since this might encourage other professional and amateur criminals to try their hand.

Financial institutions are even less willing to publicize or encourage discussion of computer-based embezzlement and related crimes. Whereas almost everyone knows, at least in theory, how to rob a bank at gunpoint or how to kite a check, the strategies for computer crimes are far more complex, more numerous, and more diverse, and are based on knowledge of new technology as yet not widely available. The new breed of criminal often attacks vulnerabilities that the institution and its management did not know existed, and often creates or discovers avenues for theft (or maliciousness) that are specific to the institution's computer systems and programs. Clearly it would be unwise to disseminate this information to other potential offenders by public discussion. Moreover, there is a strong element of gamesmanship in some computer crimes. Institutions (and the police) are not inclined to reward the offender with public notoriety that may encourage others to try to beat the system.

Thus, there is considerable motivation, in some cases at least, for not reporting or prosecuting EFT crimes, whether petty or grandiose. In addition, formal reporting systems may not have appropriate categories for identifying EFT crimes as such. These and other factors have resulted in a paucity of information about the extent of EFT security violations, and about effective strategies and technologies for preventing such violations.

Both law enforcement agencies and financial institutions would benefit from better information to increase their capability to prevent, detect, and solve EFT crimes and to apprehend and prosecute perpetrators. The public also is entitled to know the extent of risk in selecting and contracting for EFT services, and would perhaps benefit from additional education about how to use such services without creating opportunities for criminal acts. Better information would allow Congress and State legislatures to assess more effectively the need for new or modified legislation to deal with EFT security, and to build a constituency for such legislation if it becomes necessary. Such information might also stimulate the development of improved technology for security. A possible danger is that information about and wide public discussion of EFT security problems might contribute to an increase in criminal activity.

Relationship of Security to Privacy and Equity

The question of EFT security is closely related to the concerns of privacy and equity. Because information about individual customers and their transactions, which in paper-based payment systems is either not recorded or is dispersed throughout the system, is more easily aggregated and easier to access in computer-based EFT processes, privacy for the user has become a matter of public concern. Users want to be assured of the confidentiality of this information—assured that it will be aggregated and used only for purposes integral to the payment system and necessary to the carrying out of the transactions as intended by the customer. This assurance rests on confidence both in the intent of the financial institution, and in its ability to protect the information and limit access to the institution's authorized agents. If security is breached, the institution cannot provide this protection and the user's privacy may be violated. It should also be noted that some means of increasing security (e.g., audit trails) increase the possibility that privacy may be infringed because additional copies of data are created at various points in the system. Security then must be provided at more points in the system.

The relationship between security and equity is even more subtle and more equivocal. When transactions are handled and supervised by officials and employees of a financial institution, there is an element of real-time personal judgment involved that disappears when the customer interacts directly with an EFT device. A bank teller, for example, approves a withdrawal or cashes a third-party check for an unknown individual partly on the basis of established identification or other credentials and partly on trained judgment of the individual based on appearance and other factors. Where there is judgment there is also the opportunity for discrimination or prejudice.

On the other hand, EFT devices treat as equals anyone with an acceptable access card, validated credit card, etc., and do not discriminate between regular customers and purse-snatchers. At the same time, the movement toward impersonal electronic systems may create new credential requirements that will make it more difficult for some people (e.g., the poor, the young, foreign visitors) to gain initial access to EFT services.

Chapter 5 References

1. Some studies have concluded that these vulnerabilities are often overstated. *See*, for example, Kranzley & Co., *The Analysis of Certain Potential Threats to EFT System Sanctity* (conducted for the Electronic Industries Foundation under contract to the Office of Telecommunications Policy: December 1976); Federal Deposit Insurance Corporation, *Introduction to EFT Security* (August 1976); The Mitre Corp., *Study of the Vulnerability of Electronic Communication Systems to Electronic Interception* (conducted for the Office of Telecommunications Policy, January 1977).
2. Leonard Krauss and Aileen MacGahan, *Computer Fraud and Countermeasures* (Englewood Cliffs, N.J.: Prentice Hall, 1979), p. 12.
3. Edward H. Coughran, *Crime by Computer*, (University of California San Diego Computer Center: 1976), p. 24.
4. Ward v. Superior Court, 3 CLSR 206.
5. S240, Federal Computer Systems Protection Act, January 1979.
6. Telecommunications Systems to Unauthorized Use (1977), p. 11. Also FDIC, op. cit., pp. 7-8.
7. Ibid.
8. Ibid.

9. *American Banker*, Dec. 7, 1978.
10. "ATM Usage Surges During Snowstorms," *EFT Digest*, March/April 1978.
11. *Science*: "Nuclear Pulse (I): Awakening to the Chaos Factor," May 29, 1981, p. 1009; "Nuclear Pulse (II): Ensuring Delivery of the Doomsday Signal," June 5, 1981; "Nuclear Pulse (III): Playing a Wild Card," June 12, 1981, p. 1248.
12. Donn Parker, Stanford Research Institute, in presentation to California Task Force on EFT, Feb. 20, 1978.
13. American Bankers Association, *Results of an ATM Security Survey* (June 1976).
14. Comments issued by Federal Reserve on Regulation E, Mar. 30, 1979.
15. Ibid.
16. Linda Fenner Zimmer, *Cash Dispensers and Automated Tellers: Fourth Status Report* (Park Ridge, N.J., 1977) p. 239.
17. "PIN Systems Emerge as a Better Idea," *Savings and Loan News*, June 1978, pp. 98-100. *Also* "Security Approaches When the Customer Activates the System," *U.S. Banker*, Oct. 12, 1978, pp. 49, 51.
18. FDIC, *Introduction to EFT Security*, 1976, pp. 7-8.
19. Ibid., pp. 13-16.

Chapter 6

Equity in Electronic Funds Transfer

BEST AVAILABLE COPY

Chapter 6

Equity in Electronic Funds Transfer

Chapter Summary

The concept of equity includes the principles that individuals, groups, and organizations within our society should be afforded access to necessary activities and services under rational and consistent rules and procedures; that there should be no arbitrary imposition of disadvantage on some groups or the unearned enrichment of others. Implicitly, this may be taken to mean that the range of choice, rights, and benefits that consumers now enjoy should not be arbitrarily reduced. In modern society, it is essential for individuals, households, and businesses to have a mechanism for carrying out basic economic transactions (such as paying for necessary goods and services). Therefore, it is important that no segment of society—especially those already disadvantaged, such as the low-income groups or the physically handicapped—is deprived of a reliable means of making and collecting payments. In general, consumers want to preserve or enlarge their options for managing their resources in terms of using credit, scheduling payments, and shifting funds, and EFT-based financial services can and do serve these ends for some consumers.

As long as electronic funds transfer (EFT) is one of an array of alternative payment systems or sets of financial services, it does not appear that its use will result in a necessary or significant loss of equity to any group in society, nor does it appear that any group is denied access to the services and systems, except inasmuch as low income limits participation in (or need for) all financial processes. However, there may be some increased risk to individuals from undetected errors or from being less able to evaluate alternatives in choosing the most appropriate set of financial services to fit their needs. Adequate attention to consumer education, consumer advisory assistance, and designing of customer-oriented EFT devices would help to minimize these risks.

The significant benefit consumers derive from EFT could be increased if technology designers and financial service managers were attentive to diverse human needs. For example, dispersed EFT devices could be tailored to the needs of the handicapped and located to meet the needs of those whose mobility is limited. EFT offers important and obvious benefits in terms of customer convenience, reduced costs and increased productivity for financial institutions (and presumably for customers as well), and perhaps greater personal security for the user against crimes of violence and some kinds of privacy abuse.

However, if some forms of participation in EFT become mandatory or if EFT significantly displaces, reduces, or raises the costs of alternatives, this situation could change. People who do not choose to deal with banks and other financial institutions could be forced to do so, and would thus lose a degree of individual freedom. People who for various reasons are poorly equipped to use EFT systems would have their access to financial services reduced. Some communities or neighborhoods could suffer a reduction in available financial services. If this occurs, consumers would be denied the option of avoiding risks they may perceive in using EFT, and concerns about privacy, security, and accuracy of accounts would increase.

Explicit public policies to preserve some level of conventional financial services may need to be considered if market and other forces move EFT to a dominant role. Several situations could, in fact, make the use of EFT much less voluntary in the foreseeable

future. Large employers could insist on direct deposit of payrolls to employees' accounts through automated clearinghouses. Large-scale providers of services, such as utilities or mortgageholders, could pressure consumers to agree to automatic withdrawal and payment. Government agencies at all levels could move decisively toward delivery of social security and welfare checks, intergovernmental transfers, employment checks, tax refunds, and contractor payments through EFT.

What Is Equity?

The idea of equity is both cherished and elusive. It covers a multitude of different yet overlapping standards of behavior. Its content varies from society to society, and from time to time in the same society. As discussed here, equity implies:

- that there must be a generally acceptable degree of approximate equality of opportunity and access to necessary activities and services under rational and uniform rules and procedures; and
- that there must be no arbitrary imposition of disadvantage on some individuals, or unearned enrichment of others.

This working definition does not eliminate all ambiguities and contradictions, but it seems to embody the main ideas expressed in most discussions of equity.

What constitutes "necessary" activities and services is a function of social organization and changes with time. In this discussion, the term "necessary" refers to those basic economic activities for which there is no equally accessible and convenient alternative. Rules and procedures can be neither perfectly rational nor absolutely uniform, and they cannot be both at the same time.

However, using these terms it can be agreed that a license to drive an automobile (that was once important to only a few people) is now so nearly a necessity that it is denied only for overriding reasons of public safety. It can also be agreed that denial of a driver's license to someone for reasons unrelated to driving ability (e.g., physical appearance or ethnic origin) would be an arbitrary imposition of disadvantage and a denial of equity; whereas to deny a driver's license to those who are under some minimum age or who are blind is neither arbitrary nor a denial of equity. Such a denial is rational because it is based on a consideration appropriate to the activity in relation to the public interest, i.e., safety. The former categories are irrational because there is no logical or necessary connection between such characteristics and driving an automobile.

In many definitions of equity there is a third and somewhat more controversial element that may best be stated negatively:

- a reduction of equity is perceived when the range of existing, well-established choices or options is significantly reduced to certain population subgroups.

The differential reduction or elimination of options is often perceived as an inequity whether it results from a Government order or the working of market forces. For example, when the wide availability of automobiles led to the demise of urban transit systems and rail passenger services, a serious disadvantage was imposed on those who are too poor, old, young, or handicapped to drive. This may well be termed a loss of equity and, recognizing this, governments have sometimes intervened to preserve these services as alternatives to automobile use.

A government fiat, rather than market forces, may bring about the elimination of existing options. For example, the banning of residential air-conditioning—for instance, in a region suffering a severe and prolonged shortfall in electricity generation—might be perceived as a loss of equity even by those

who have been unable, or have not chosen, to exercise the option of buying air-conditioning.

The present discussion focuses on the way in which EFT might narrow consumer options for carrying out financial transactions, although this might better be called a potential social disbenefit rather than a loss of equity. Gross disparity in income may or may not be defined as inequity, but in any case it is not substantially affected by EFT and therefore is not pertinent to the present discussion. However, the extent to which services are accessible to all who seek to use them under rational and relatively uniform rules and procedures is important. Equitable access to EFT services may be a relatively insignificant issue at present. However, its importance would increase greatly should EFT services displace other payment systems to any major extent, thus making conventional payment systems less acceptable, more costly, or less readily available.

Equity in Payment Systems

EFT technology and services can change the relationships between providers and consumers of financial services, and the relationships among the providers as well. It has the potential for changing the relative acceptability of various forms of payment. Such social changes may inadvertently impose disadvantages or inequities on some segments of the population, on the general public, or on some institutional participants in the financial exchange system.

Special segments of the population whose status with regard to EFT should be examined carefully are those who are or often have been placed at a disadvantage in other social processes and institutions—racial and ethnic minorities, the poor, females, the aged, the handicapped, and those without acknowledged and established economic status.

In terms of the mainstream consumers of financial services, there have been concerns about equity with regard to the effect of EFT on:

- the acceptability of alternative methods of payment, and hence the preservation of a full range of choice between payment systems and financial services;
- the ability of the consumer to manage financial affairs, control the timing of purchases and payments, and have access to credit;
- allocation of the costs of financial services; and
- the ability of the consumer to guard against errors.

EFT Equity and the Socially Disadvantaged

The question at issue here is whether EFT technologies and services would increase or decrease the social disadvantages already suffered by some segments of society. It arises because social institutions and processes designed to meet the needs and wishes of mainstream, dominant population groups all too often are unsuited to the needs of peripheral groups, and thereby unnecessarily add to their problems in carrying out basic human and social functions.

It is possible that some EFT systems and services that are dispersed or decentralized can be tailored to the needs of special groups or communities, thus alleviating some of their problems with standardized service delivery systems. Also, since EFT services

are depersonalized they may eliminate some of the subtle, deeply embedded forms of discrimination to which such groups are subjected. It is important to keep in mind that potential sources of inequity for special groups may be balanced to some extent by beneficial effects, especially if the providers of EFT services are alert to the possibilities of using EFT capabilities to meet social needs. For example, automated teller machines (ATMs) and point-of-sale (POS) terminals in nursing homes and communities for retired people can allow some people to retain a degree of independence in managing their affairs that they might otherwise lose.

The Poor

Based on the results of one 1977 survey, it is estimated that 81 percent of U.S. adults have checking accounts (1). Most of those who do not are people with very low incomes. The best evidence is that 35 percent of those who do not have checking accounts are poor, i.e., they earn less than $5,000 annually or live on social security benefits or welfare. Another 58 percent are skilled or semiskilled workers earning $7,000 to $15,000 annually (2). It is not entirely clear whether these people do not choose to have accounts, or whether they are somehow denied access to checking accounts.

Those who do not deal with depository institutions must rely on currency and money orders, one of the most costly ways of effecting payment. Supermarkets, taverns, and check-cashing booths will convert payroll or social security checks to cash, often for a relatively large fee, and money orders can be used to send payments safely through the mail. These appear to meet the needs of many people. However, changes taking place in the financial services industry make it impossible to assume a priori that currency and money orders will continue to constitute a minimally acceptable set of payment services.

The Department of the Treasury is encouraging recipients of transfer payments to accept direct deposit of benefits (3). While there may be many advantages to recipients in doing so (such as reduced threat of mailbox robbery and reduced transaction costs), certain disadvantages may be perceived. Some transfer payment recipients may believe their privacy is threatened, or may be intimidated by having to deal with impersonal institutions or systems. Mobility may be a problem. At any rate, a forced "choice" can be considered an inequity if imposed on some but not all population subgroups. People may also suffer a loss in equity if they are encouraged or pressured to become users of noncash payment systems or EFT systems, but are given little assistance in becoming familiar with the systems, with the various choices of services, and with mechanisms for correcting errors or detecting fraud.

A related question is whether ATMs and other dispersed forms of EFT systems will be placed in low income neighborhoods, which are also often high crime areas. In some locations, it may be impractical or impossible to assure the security of the devices or of the customers using them. A diminution of traditional neighborhood banks in favor of EFT services, coupled with a reluctance to locate EFT services in high crime areas, could place a severe hardship on some low income population subgroups.

The Elderly

Elderly people often derive their income from a variety of sources—one or more pensions, social security, savings, family contributions, or part-time work. They may, therefore, have need of a variety of financial services and exercise them frequently. The convenience of EFT systems can be beneficial to the elderly, especially if the need to travel to banks outside the immediate neighborhood is reduced. It has been suggested that EFT systems are popular in some communities that have a large population of retired people. At the same time, many of the elderly are also poor and suffer some of the disadvantages already described. They may be intimidated by their unfamiliarity with

complex systems or living in neighborhoods where such services are not available. Progressive failure of short-term memory, a fairly common disability of the elderly, may make it difficult for them to become familiar with new systems. Asking strangers for help with the devices is likely to expose them to fraud and victimization. For these reasons, it is important that alternative services and/or human support continue to be available.

Women

Women attempting to establish a personal credit record after some years of marriage and subsequent divorce (or widowhood) often have trouble doing so, but this does not appear to be exacerbated by EFT systems. In fact, EFT services might eliminate some of the opportunities for personal discrimination against women in obtaining financial services. Positive verification services can enhance the acceptability of noncash payments and implicitly create a positive record of fiscal responsibility.

Government regulations allow Federal administrative agencies (e.g., Internal Revenue Service and Social Security Administration) to use automated data systems to locate parents who are avoiding child support responsibilities (4). If EFT data banks could be used for this purpose, EFT could potentially confer a benefit on women insofar as husbands are most typically the missing parent and wives most typically the victimized parent. However, the social costs of such Government surveillance could be substantial.

There appear to be no significant inequities to women from a shift to EFT.

Racial/Ethnic Groups

Since EFT systems are depersonalized, they may eliminate situations where traditional financial service delivery systems may have discriminated against individuals because of race, color, ethnicity, or accent. An inadequate command of written English may present a problem, but this might be accommodated by multilingual instructions, graphics, or supplementary human support systems. Multilingual systems have already been implemented in some areas. There appear to be no important additional inequities in EFT systems for racial and ethnic minorities other than those they already experience.

The Handicapped or Disabled

The handicapped may experience a number of unavoidable difficulties with dispersed customer-oriented and customer-operated EFT systems. These are different in kind rather than in magnitude from the problems the handicapped may have with alternative systems. The visually impaired or dyslexic may have difficulty operating systems that depend on reading instructions; on the other hand, the deaf may find dealing with such systems more congenial than with human tellers. Operating ATMs or POS terminals probably takes no more muscular coordination than writing checks, and perhaps less. As long as alternative payment systems are available, EFT should impose no new disadvantage on these groups. However, should EFT displace alternative systems, some of the handicapped may be subjected to unacceptable disadvantages unless compensatory mechanisms (e.g., special human assistance) are provided.

Transitional Groups Without Recognized Financial Status

This somewhat anomalous group includes various special groups that are in transition from one socioeconomic status to another, or whose social-economic credentials are not yet established. For example, first-time workers and young professionals; students; recent retirees; immigrants; recent widows never employed; women re-entering the work force after some years as housewives; former mental patients; and former prisoners might all fall within this group. Because some EFT services require an extension of credit, and

credit approval depends heavily on credentials and long-term credit ratings, such people are at a disadvantage in procuring credit-based financial services. This disadvantage may be less significant in small, stable communities where personal knowledge of applicants overrides the lack of credentials.

The General Public as Consumers of Financial Services

The Knowledge To Choose

Money functions as a store of value and as a medium of exchange. As a store of value it is expected to retain its buying power (aside from the effects of inflation). As a medium of exchange it must be readily acceptable as a form of payment and convey value from one party to another easily and reliably. However, the acceptability of noncash payment instruments cannot always be assumed. Losses from credit card and check fraud are substantial. Many businesses will no longer accept personal checks unless the customer is known (or "looks reliable," which introduces many forms of discrimination). Others require two items of identification and often require that at least one of them be a major credit card. Alternatively, some merchants require personal identification to back up a credit card.

However, vendors know that customers are prone to buying on impulse, which is encouraged when checks and cards are accepted. The vendor also wants funds to be available as soon as possible because financing receivables represents a considerable expense. While vendors prefer to be paid at par (face value), they are willing to pay fees to organizations that authorize or guarantee checks, and to take discounts from credit card and debit card processors in order to assure payment and to speed it up.

Customers want payment instruments to be readily accepted at face value, and minimal embarrassment if a payment is refused. It has become more convenient for many people to pay by credit card than by check, especially if they are out of their local trading area. In addition, procedures may be less complex for a credit refund than for a cash refund. To the extent that merchants accept credit cards more readily than personal checks, those who have no credit cards are disadvantaged. When a check is an unacceptable instrument, it can no longer fulfill the customer's expectations of money.

However, check authorization and guarantee services are now helping to remonetize the check. The development of the debit card is providing another means of drawing upon transaction balances that should be readily acceptable to vendors. Thus, various EFT services are helping to increase the ability of transaction balances to meet the need for payment instruments that have the functional characteristics of money.

Financial management is a very personal activity. Some rely on cash almost exclusively, while others select a variety of financial services that best meet individual economic and emotional needs. Some adopt strategies that maximize the use of "free" credit and minimize the funds kept in accounts that do not earn interest, and some make payments at the last moment to obtain greatest benefit from the available funds. Financial institutions compete, therefore, by varying the structure and prices of the services they offer. The Depository Institutions Deregulation and Monetary Control Act of 1980 (5) has put banks, savings and loan associations, and credit unions on an equal footing in many regards. Nonfinancial institutions are becoming more aggressive in selling financial services. New services have been made available by the increase in EFT offerings. Many providers of financial services

are offering packages that are closely tailored to consumer needs, which may be dictated by wealth, lifestyle, and personal preference.

As a result, consumers are faced with a number of alternatives for acquiring payment services, and the number is increasing rapidly because of EFT. In order to make choices to the best advantage, the consumer must have the ability to evaluate alternatives. Not all individuals, particularly those lacking in formal education and experience in financial management, are prepared to do this. Consumer education is required, and many providers of financial services and other agencies are beginning to furnish it.

Consumers need to become familiar with five aspects of financial services:

1. costs;
2. the mechanics of using such services;
3. the benefits that are offered;
4. the obligations and responsibilities that are accepted when participating in each service, such as the ways to safeguard one's own account (e.g., discretion in use of personal identification number); and
5. their rights as consumers, and especially the methods for identifying, challenging, and correcting errors.

The sophistication required to select a set of financial services most appropriate for one's needs is therefore growing, and is probably outpacing the consumer education that has been made available. If the industry is trying to tailor services to the needs of most of its customers, the level of skills required to select an optimal mix of services may be unrealistically high for some population subgroups.

The Preservation of Options

There is also concern that in the future there may be an implicit but real compulsion to use EFT. All people require a means for effecting payment. Currency meets these needs for face-to-face exchanges, and money orders provide a reasonably convenient (though relatively expensive) means for safely sending payments through the mails. Together, cash and money orders meet all of the needs for executing the most basic minimum set of transactions, and access is virtually universal. More sophisticated payment services are generally available to those who require them.

The law does not allow creditors to require the use of EFT in making payments. However, some mortgagees, for example, strongly encourage applicants to agree to automatic deduction of payments from their accounts. At present, there is no legal prohibition against an employer requiring employees to accept payment of wages by direct deposit, although the employer may not insist on deposit in a specific depository institution. Government agencies are encouraging social security recipients to accept direct deposit. In the future, it is possible that Government payrolls and social security benefits may all be subjected to direct deposit in the interests of reducing Government costs and protecting recipients against theft. The Treasury Department has considered requiring distillers to submit taxes on alcoholic beverages by EFT and is considering delivering tax refunds by this method (6). Several major industrial firms already require employees to accept pay by direct deposit. Thus, for significant numbers of people there is very real pressure to use EFT at least for receiving funds. This in turn creates the need to establish an account with a service provider.

A second way in which EFT services may become more compulsory is by simple market displacement of alternative systems. Because of their inherent advantages to financial institutions, EFT systems could discourage the maintenance of older services. Under some conditions, banks might not be built in new communities and neighborhoods and older banks may not be replaced as buildings become obsolete. Dispersed ATMs and POS terminals would be much less costly. Credit cards could be withdrawn or priced to be

noncompetitive in favor of debit cards. A cascading series of such effects, driven only by mass market forces, is conceivable. In the same way, the automobile displaced local mass transit and the airplane replaced rail passenger service. Even though some, and possibly many, people may prefer conventional alternatives, there is no guarantee that those alternatives will be maintained.

For example, service providers may shorten lobby hours when sufficient ATMs are available, or may reduce significantly the number of tellers in the lobby. Check-handling charges may go up to compensate for lost economies of scale. This kind of evolution is precisely the hallmark and advantage of a relatively free market, but each such change causes perceived disadvantages to some people who do not or cannot go along with the preferences of the majority. However, it must be recognized that in a free market, services will disappear as they replaced by those that are preferable to the majority. To the extent that EFT displaces alternatives, equal access to EFT services becomes more important, as do other concerns such as privacy and security. As long as consumers have a practical choice, they cannot be subjected unwillingly to perceived risks. In addition, financial institutions will take consumer concerns seriously and devise corrective measures (if needed) to avoid losing customers.

The Economics of Payment Systems

Concerns about privacy and security are stimulated by the nature of EFT technology. Concerns about social equity are much less closely tied to technology and tend to derive from the way in which managerial decisions are made by providers of financial services. EFT technology creates new options for the institutions, but the decision criteria are business-oriented and technology-structured.

The location and timing of services are decided by geographic, economic, and demographic factors, but not necessarily on the basis of whether alternative services and institutions are available to consumers in those areas. Price schedules are established with management deciding whether a service will be subsidized and for how long. Loss leaders are widely used in business for good economic reasons. Managerial decisions to use technology to supplement or replace human resources in delivery of services are driven by cost and competitive considerations. Since prices to consumers should reflect the cost of providing services, it is reasonable to expect that fee structures will develop that reflect the lower costs of EFT services. However, this differential may be increased where providers subsidize EFT ventures with revenues from existing services.

Customers then may be expected to tolerate some inconvenience or additional costs in the relatively rare cases when a transaction requires a human teller; this will become a specialized rather than a mass-market service. But those who must rely on human tellers for some transactions—e.g., the blind—may find that the times and places where tellers are available have been markedly decreased. Alternatively, they may find that telephone transfers and ATMs with Braille keys and voice response may be available to meet their needs.

Some critics point out that the market for financial services does not meet the assumptions of a purely competitive market in which all economic and social costs are recognized and services are allocated in a way that is responsive to societal needs. Highly efficient markets are not necessarily equitable providers of goods and services. Some consumers may be out of the mainstream and, if few in number and/or expensive to provide for, may be left out for all practical purposes if the market works efficiently. With a social activity that is so essential to adequate functioning in our society as is the performance of financial transactions, relative deprivation of access can become a serious social issue.

There is evidence that EFT can substantially reduce the time and money that both consumers and businesses spend paying bills, handling checks, and collecting payments. A State of California study noted in 1979: "The savings which EFT can bring in consumers' time and in processing costs for depository institutions have been projected to be more than $1 billion per year nationwide . . ." (7). It also concluded that EFT could reduce by substantial amounts the total expenses for credit card operations (which in 1979 were running as high as 10 to 15 percent of outstanding amounts). EFT can also reduce the loss of revenues suffered by merchants due to the float between receipt of a customer's check and payment by a bank. There is also concern as to whether the savings from use of EFT will be passed on to consumers in the form of lower checking account service charges and credit card interest charges, or whether the users of these alternative systems are involuntarily paying the costs of adding EFT systems that they themselves do not choose to use.

A more specific but less obvious issue involves those potential situations (discussed above) in which people who by choice have no depository relationship might be forced to establish one in order to receive social program benefits (or payroll checks). These accounts could quickly become zero balance accounts from which the customer withdraws all funds as quickly as available. Arguments can be made that

- the (involuntary) customer should pay the costs of the account since he or she is the beneficiary, enjoying less danger of theft and possibly higher social status thereby;
- the financial institution should absorb the costs because it can, over time, sell the customer additional services with minimum effort; and
- the employer/agency should pay the cost because it is the party that initiated the requirement, presumably to reduce its own costs.

There may be alternative methods for making funds paid by direct deposit available to the recipient; for example, an employee or welfare recipient could be provided drawing rights against a common account to which salaries of all employees, or benefits to all recipients, are credited. Specialized institutions could be established through which payments could be funneled.

Personal Money Management

Individuals use a variety of strategies to extract the maximum benefit from personal and household funds, or, more commonly, to stretch limited incomes to cover their family's needs. Dependence on daily, weekly, or monthly wages (or benefits checks) allows only limited flexibility. Many people increase this small margin of maneuverability by using retail credit, which allows them to make a large purchase and pay over a long period, or to lump together many small purchases and pay varying amounts on a more or less regular schedule. One of the bargaining points of any commercial transaction is, in fact, the timing and method of payment.

A credit card is a convenient method of credit for a wide range of goods, services, vendors, and locations, and is acceptable in many places and situations where personal checks are not. Other forms of credit are also used as a bargaining chip on both sides of a transaction. Discounts are given for payment on delivery or within a specified time; interest or payments may be deferred ("Buy in time for Christmas—no payments due until February!"). People also use less formal forms of credit, e.g., writing a check against a zero balance on Friday, knowing that a paycheck will be deposited on Monday to cover it.

The cost of supporting lines of credit and servicing credit accounts and usury limits may cause financial institutions to emphasize the debit card over the credit card. Credit cards permit the consumer to control the timing of disbursements, but the cost of credit to the consumer is likely to increase.

Debit cards, on the other hand, reduce people's control over the timing of payments. They also limit the ability to withhold payment if the purchase is unsatisfactory. The question of reversibility, or the right to stop payment, is a serious concern for consumers. Some argue that the use of a card is the functional equivalent of cash and is not reversible; others claim that it is the functional equivalent of a check and that stop payment orders should be permitted. Reversibility is especially important with preauthorized payments. The Electronic Funds Transfer Act of 1978 provides that customers can place a stop on preauthorized payments, but only up to 3 business days before the transaction is due. Some States (Wisconsin, Michigan, New Mexico) provide more extensive reversibility rights.

Liability

According to the Electronic Funds Transfer Act of 1978, financial institutions are liable for damages caused by their failure to transfer funds as instructed by the customer, unless the failure was caused by an "act of God" beyond the institution's control. This does not directly answer the question of whether an electrical blackout is such an "act of God" or whether the institution should provide sufficient backup to prevent such failures. It also does not address the liability of third parties (e.g., a merchant with a POS terminal). If the card is used fraudulently, consumer liability varies with the degree to which his/her actions contributed to the loss.

Customer Vulnerability to Errors

EFT customers bear somewhat greater responsibility for detecting and correcting errors than with payment systems relying on paper instruments and a full panoply of human support services. At the same time, the various statements and printouts provided to the customer are more complicated and less familiar than a batch of returned checks in one's own handwriting. Procedures for reconciling errors may appear formidable. At least in the early stages of developing familiarity with EFT systems (which in any case vary widely and are constantly changing), customers may tend to be intimidated by the devices and believe themselves more likely to be in error than the system; they may hesitate to challenge the accuracy of any printout statement and fear embarrassment if caught in a failure to understand it. Attention to consumer education would probably cause these problems to diminish as experience with EFT increases.

In Conclusion

There appear to be few reductions in equity inherent in EFT systems for socially disadvantaged groups, as long as a full range of alternative payment systems and financial service delivery systems continue. In this situation, EFT expands the range of services from which special groups may choose, and thus increases the possibility of finding delivery mechanisms that better accommodate their needs. In a few cases, designing EFT systems to meet specialized requirements would be relatively simple and would deliver significant benefits to groups that are disadvantaged at present. However, in the future, if EFT displaces conventional alternatives in certain neighborhoods, communities, or regions (or replaces them completely), socially disadvantaged groups may suffer significant additional restrictions on their ability to function in society. The largest socially disadvantaged group, the poor (which includes many with other disadvantages as well), could be maneuvered into accepting new payment mechanisms that they would not choose voluntarily.

EFT and equity raise important questions for consumers and the public at large. Will

consumers be given sufficient information, in terms they can readily understand, to choose the optimum mix of services? Will the costs of alternative financial services and payment systems rise or fall because of EFT? Will their ability and maneuverability to manage personal finances through formal and informal means increase or diminish? Will they become more or less vulnerable to bank errors and system failures that they may be unable to detect or prove? Will they retain, both in principle and in practice, full freedom to use or not to use EFT systems and services?

The importance of these questions and issues increases as EFT becomes more widespread. It is possible, even likely, that the lower cost of EFT services may lead to their replacing older forms of financial services, at least sufficiently to make the traditional services and systems less readily available or more costly. Because access to basic economic activities and functions is essential to life in modern society, any reduction in equity for any group within society would be a matter of public interest and concern.

Chapter 6 References

1. Payment Systems, Inc., *Payment Systems Perspectives '78, A Nationwide Survey of Consumer Views on the Changing Payment Services* (Atlanta, Ga.: April 1978).
2. R. F. Schlax and S. J. Levy, *A Quantitative Analysis of Why People Do Not Have Checking Accounts* (Chicago: Bank Marketing Assoc., 1971).
3. Working Paper A: Imperial Computer Services, *Electronic Funds Transfer: The Policy Issues* (May 1979), p. 60ff; *see also* "Automated Clearing House Network, Its Progress, Problems, Potential," *Banking*, March 1979.
4. 45 CFR 302.71.
5. Public Law 96-221.
6. Working Paper A, p. 60ff.
7. *Electronic Funds Transfer: A Guide for Public Policy*, the Final Report of the Interagency Task Force on EFT, State of California (March 1979), p. viii.

Appendixes

BEST AVAILABLE COPY

Appendix A

Other Questions and Issues Concerning Electronic Funds Transfer

Appendix Summary

Privacy, security, and equity in electronic funds transfer (EFT)—the focus of this background paper—are only three of the many issue areas concerning EFT that are as yet unresolved.

One other cluster of major questions points to two fundamental and related issues: 1) Will the future usefulness and cost effectiveness of EFT be limited unless Federal and State laws are changed to allow EFT to operate across jurisdictional boundaries, under uniform rules and procedures? 2) Are the risks to small financial institutions and to a decentralized and disaggregated financial services industry so large that existing restrictions should be maintained and perhaps strengthened?

A second group of questions has received so little attention that they have yet to be articulated as public policy issues. These concern possible consequences of EFT for the Nation as a whole, aside from its financial structures. Some of these questions involve the effects of large-scale EFT systems on national welfare and national security. Other, broader questions relate to changes in the number and nature of jobs in the future. Many of the broad indirect effects of EFT perhaps have not yet been anticipated.

A third group of questions relates to the effects of EFT on consumers of financial services, and equally important, on those in society who are not (or not yet) consumers of financial services. These include issues concerning the role of the Federal Government as a user, regulator, and/or provider of EFT services, as well as the issues of privacy, security, and equity discussed in chapters 4, 5, and 6 of this background paper.

The future effects of wide-scale adoption of EFT are, in fact, difficult to forecast. Much depends on the relative speed with which EFT is adopted, the level of use it finally achieves, and the changes that will occur in these and alternative technologies over time. The use of EFT could eventually be widespread, almost completely replacing some alternative means of delivering financial services and carrying out transactions.

This makes it important that attention be paid to the full range of potential impacts on society, as well as to perceived areas of concern such as privacy, security, and equity. There has been as yet no comprehensive, exhaustive search for such downstream effects.

EFT and the Structure of the Financial Services Industry

EFT systems and services affect the relationships between financial services and among providers of financial services. The changes this might bring about in the financial services industries, and whether any of these changes will significantly affect the public interest, raise a number of questions and issues.

Should automated teller machines (ATMs) and point-of-sale (POS) terminals continue to be defined as branch banks?

In January 1974, the Federal Home Loan Bank Board (FHLBB), which regulates savings and loan associations (S&Ls), allowed the Federal Savings and Loan Associations of Lincoln, Nebr., to place EFT terminals in the Hinky Dinky Supermarkets. The terminals allowed customers, with the assistance of the supermarket personnel, to make deposits or withdrawals from their savings accounts and to cash checks. Although financial institutions had been experimenting with EFT, this event shocked the industry. It involved S&Ls in an activity that looked very much like banking, and it made merchants look very much like bank officers. The Comptroller of the Currency immediately ruled that ATMs and POSs were not branch banks so that banks could deploy terminals; otherwise commercial banks in many places would be unable to compete with S&Ls (1). However, this finding was reversed in a court case that was carried to the Supreme Court (2).

The 1927 McFadden Act defined a branch bank as a location where deposits were received, checks paid, and money lent. The Banking Act of 1933 allowed federally chartered banks to have branches only where State banks were authorized to branch under State law.

Generally, only commercial banks are subjected to branching restrictions. Federally chartered thrift institutions are not so restricted, and Federal S&Ls may have branches if approved by FHLBB. However, the FHLBB usually has adhered to State or metropolitan area boundaries in allowing branches, although a recent FHLBB policy permits deployment of remote service units across State lines. Illinois and West Virginia completely forbid branching, although Illinois has passed legislation that permits the phased deployment of ATMs.

Strong opposition to branch banking developed at the turn of the century. This was based on fear that it would lead to industry concentration; place small, independent or unit banks at a disadvantage; and deprive small communities of access to credit and financial services (3). Proponents of branch banking argue that it stabilizes cash flow, prevents bank failures, provides an expanded range of services in small communities and neighborhoods, improves local sources of credit, generates economies of scale (thus reducing consumer costs), and meets the needs of a highly mobile population.

Since ATMs and POSs are defined as branch banks, they are subject to the same approval criteria as "brick and mortar" branches. This places commercial banks at a disadvantage compared with other financial institutions. The National Commission on Electronic Funds Transfer (NCEFT) therefore recommended changes in legislation. Illinois, a unit banking State, has now passed legislation that permits the phased deployment of offsite ATMs, although "brick and mortar" branches are still prohibited (4).

EFT devices could be exempted from laws restricting branch banking. Alternatively, States could authorize their use statewide and enter into reciprocal agreements with other States for out-of-State utilization. Or the Federal Government could preempt State action and authorize EFT devices nationwide. Such proposals have been meeting strong opposition from some small banks, from consumer groups who fear the growth of banking oligopoly, and from many States opposed to preemption (5). However, as already described in chapter 3, many nondepository financial institutions are developing interstate EFT services.

Should shared EFT networks be permitted, made mandatory, or be prohibited?

Small institutions may be unable to enter the EFT market unless they have access to EFT networks. Because investment costs for EFT networks are high and the economies of scale are large, small institutions want to be able to establish EFT networks through joint ventures or cooperative efforts. This immediately raises questions about antitrust rules. Soon after the first offsite ATMs were placed in 1974, 20 States responded to this concern by passing mandatory sharing laws under which any EFT network established must grant access to any qualified institution seeking it. Nine States have "permissive" sharing laws. Some of the shared (or proprietary) systems have "like" members (e.g., all S&L associations) and some have unlike members (6).

Concerns then are raised about whether some shared systems are so inclusive as to dominate their market and preclude new entries, thus foreclosing further innovation and development. Antitrust law is meant to encourage competition among firms, rather than joint ventures; but it allows for cases where risk is greater and/or economies of scale are greater than individual firms can accommodate (7).

Some shared EFT networks have become very large. The Nebraska Electronic Transfer System (NETS) included 86 percent of all commercial banks in the State, and the Department of Justice brought action against it as anticompetitive (8). The Department of Justice issued a letter warning that automated clearing house (ACH) associations had established exclusionary policies that discriminated against some classes of institutions (9). As a result, ACHs have been directed to provide service to all depository institutions (10).

NCEFT recommended that sharing or nonsharing be left to market force determinants, subject to antitrust proceedings when reasonable bounds were exceeded. The policy issues involved are the following:

- What is the best way to assure access for small firms, yet provide the maximum competition that markets can support?
- Should shared networks that dominate a market area be regulated as a public utility?
- Should this be decided on a State-by-State basis?

Should foreign financial institutions have unrestricted entry into the American EFT market?

Foreign banks may establish branches in multiple States, while an American bank may not buy a bank or establish a branch in another State. Some argue that this puts American banks at a relative disadvantage. If foreign banks choose to expand the number of States in which they operate, and especially if they expand EFT services, Congress will be urged to address this issue.

Might EFT change the structure of the financial services industry and, in so doing, reduce the viability of small financial institutions?

There are about 40,000 depository institutions in the United States, most of which are small. In 1979, the largest bank had about $62 billion in assets, and the bank that ranked 132 had about $1 billion (11). There is concern that EFT may place small institutions at a greater disadvantage because:

1. of the capital costs of the EFT technology,
2. EFT may lead to a change in the laws restricting branch banking, or
3. small banks cannot gain access to important EFT communication networks.

There is no evidence that this is happening at the present time. EFT technologies, such as ATMs, are becoming less expensive while labor costs continue to rise. Some observers say that small institutions are adopting EFT systems more rapidly than larger institutions. Changes in branch banking laws, however, could change the situation in the future. The viability of small financial institutions may also be threatened, perhaps to a greater degree, by other factors such as high interest rates, deregulation, and competition from large financial services conglomerates. For example, these factors are contributing to a significant increase in the number of mergers among savings and loan institutions.

EFT and the National Welfare

Aside from the potential impacts on individuals and groups, and on payment systems and the financial services industries, there are potential impacts of a more general nature that should be considered. One is the dependence on a complex technological system or systems for functions that are essential to the Nation's welfare and security. Another is the effects on nonfinancial businesses and commercial activities and on employment throughout all economic sectors. A third is the impact on Government itself and on the delivery of Government services.

Would increased dependence on EFT create increased vulnerability to national enemies, terrorists, or natural disasters?

When a community or society becomes dependent on a complex technological system and allows older, perhaps less efficient alternatives to disappear, any failure or disruption of the system can create a crisis—sometimes a catastrophe. A city can be thrown into turmoil by disruption of a number of systems, such as potable water supply, waste pickup, sanitation, telephone, transit, etc. But an electrical blackout has more serious and immediate effects, and if citywide or prolonged it can be disastrous. There are few or no practical alternatives left for most of the functions performed by electricity, at least in the short run. Even at the national level, any disruption of systems on which people have become dependent (such as air travel, mail service, or petroleum delivery) can cause severe economic loss and personal suffering.

Complex systems can be disrupted for many reasons, such as normal component failure, human error, sabotage, or a natural disaster. The question is whether the Nation as a whole can be put at risk or coerced by the threat of disruption of EFT systems by, for example, violent political dissent, terrorism, or attack by external enemies (12). (See table A-1.)

Terrorists might attack EFT systems for several rather different reasons. One is to gain funds (and conceivably data) to support revolutionary activities. Other, more direct motivations might be: 1) to disrupt a system essential to the economic functioning of a community or region in order to demonstrate the power, commitment, and ruthlessness of a terrorist group, or 2) to lend

Table A-1.—A Comparison of EFT Threat Levels by Source of Threat

	Past threat: all computer crime	Future threat: massive EFT losses
Amateur white-collar criminals	High	Low
Deranged individuals	Low	Medium
Unethical business enterprises	High	High
Career criminals	Low	Low
Organized criminal groups	Low	Medium
Extreme economic advocates	Low	Medium
Extreme political advocates	Medium	High
Foreign powers	Low	High

SOURCE: Donn B. Parker, SRI International, in "The Potential Effects of Electronic Funds Transfer Systems on National Security," Session 19, International Conference on Computer Communication, Atlanta, Ga., 1980.

credibility to their threats in order to force governments to take some action (e.g., to release "political" prisoners or pay a ransom).

It is possible to "harden" the security of EFT systems and/or provide backup computer capability as such threats materialize. However, this would increase costs and thus slow the adoption of EFT systems. It is unlikely to be undertaken on a major scale unless and until the threat to national security has been demonstrated to be real.

How would nonfinancial businesses and general employment levels be affected by widespread use of EFT?

Little systematic attention has been given to this question. It is clear that all businesses—not merely financial institutions—will feel the impact of EFT; indeed some are already affected. Many, and quite possibly most, businesses will eventually use EFT for some or all of the following functions:

- automatic deposit of payrolls;
- automatic registration and cataloging of accounts receivable by the bank;
- payment of bills; and
- general management of financial assets.

It is reasonable to assume that the clerical work force will be affected, both by microeffects (on the number and kinds of office workers needed by individual businesses) and by macroeffects (on the kinds of workers in demand and on the level of employment in some categories of jobs, on a national level). The exact nature and degree of such changes is poorly understood at present. EFT will tend to reduce the number of clerical jobs, but how much is still unclear.

One organization that may experience adverse effects is the U.S. Postal Service. Much of the volume of first class mail is related to financial transactions, probably about 60 to 70 percent (13). Roughly 50 percent of postal revenues are generated by first class mail (14). The costs of handling this category of mail are relatively insensitive to volume; large decreases in the volume of first class mail handled would have serious consequences for the financial viability of the Postal Service as now constituted.

Some EFT services would tend to increase the volume of payments-related mail; e.g., a switch from passbook savings to services where monthly printed statements must be sent to customers. However, this is likely to be far outweighed over time by the negative impacts of other EFT services, such as automatic bill paying and the direct deposit of paychecks and social service checks. Even monthly statements may eventually be sent electronically to business computers or home terminals for printout onsite.

The Government Role in EFT

Another controversial issue is the question of the appropriate role for the Federal Government. Federal agencies will continue to be among the largest users of EFT services. What, then, are the potential impacts of EFT on delivery of Government services, and what might be the secondary impacts of reliance on EFT? Because payment systems are intimately related to the integrity and health of the Nation's economy and social well-being, their proper functioning is a matter of public interest and national concern. How should responsibility for their monitoring and regulation be allocated among Federal, State, and local governments and industry self-regulation? A Federal entity, the Federal Reserve Board, now operates ACHs, a crucial link in the developing network of EFT services. Is this a necessary and appropriate role? Should it be expanded or contracted?

Thus, the Federal Government has at least three roles in relation to EFT—user, regulator, and provider. Each role causes some concern or controversy on the part of some other actors in EFT development. The question of possible abuse of EFT systems for Government surveillance is considered in chapter 4.

As a user of EFT, the Federal Government already makes a significant portion of social security payments through EFT (about 30 percent in 1980), as well as some payroll deposits (15). Potentially all payrolls, retirement benefits, unemployment checks, veterans benefits, disbursements to State and local governments, and payments to contractors could be handled through EFT. Federal law now prohibits mandatory automatic deposit of benefit checks into a depository institution, but the costs of maintaining dual-payment systems will eventually have to be balanced against these other potential social costs.

The financial services industry generally would prefer a minimum of regulation, except that each category of financial institution wishes its competitive position vis-a-vis other kinds of institutions to be protected. Because States may have different policy positions toward such issues as branching and sharing of EFT networks, they are reluctant, for the most part, to have their regulatory responsibilities preempted by Federal ac-

tion. Dual systems of regulation can cause problems for the industry in the future, but many smaller institutions are fearful that Federal preemption would void State laws designed to protect them against any tendency toward concentration in the financial services industry.

Many consumer groups, on the other hand, want stronger Federal legislation in the areas of privacy, security, and equity. Civil libertarians argue for stronger laws in these areas to limit access to data for the Federal Government, as well as for State and local governments and private sector organizations. Some observers believe that the Federal Government has a responsibility to aggressively protect EFT systems from potential abuse or illegitimate and/or illegal use. Extension of the Bank Protection Act and Regulation P to cover EFT systems and services has been suggested.

The Federal Reserve System (FRS) now operates all but one of the 32 ACHs. This developed as an extension of the FRS role in operating a check-clearing network, an activity based on the Federal Reserve Act of 1913. This act was passed following the financial crisis of 1907 when it became clear that the private sector was not performing this task effectively (16). FRS provided the check-clearing service in a cost-effective manner, assuring access to the system for all depository institutions (17). This has also been true of ACH operations.

In 1978, the regional ACHs were linked by a communication system. FRS and the American Bankers Association have developed standards that will permit ACHs to clear customer-initiated individual entries originated by telephone, ATM, or POS (18). FRS is now implementing a new communication network that will carry ACH and Fedwire transactions as well as administrative messages. These activities suggest that FRS intends to maintain a major role as a provider of EFT services (19).

FRS became the major ACH service provider because of its early development of and support for ACHs and because its services were supplied for the most part without charge to its members. However, the Financial Institutions Deregulation and Monetary Control Act of 1980 (20) forced FRS to charge for its services.

Nevertheless, some financial institutions and associations object to FRS as a provider of EFT services, claiming that it unnecessarily competes with private sector institutions, and that the inevitability of cost-subsidy will discourage private entry. Critics also say that the FRS role as a provider of services conflicts with its role as regulator of financial service providers, and that it provides a dangerous invitation to Government surveillance (21).

On the other side, including the National Commission on Electronic Funds Transfer, are those who argue that the clearinghouse function is one that should be considered a natural monopoly because the economies of scale are so large; yet the investment required makes it impractical for any one private sector organization to fulfill this role as efficiently as can FRS (22). In addition, they argue, FRS can be counted on to provide service to all, i.e., to guarantee equity of access.

Appendix A References

1. Working Paper A. Imperial Computer Services, *Electronic Funds Transfer: The Policy Issues* (May 1979), p. 14.
2. *Independent Bankers Association of America* v. *Smith*, No. 75-1786 (D.C. Cir., Mar. 27, 1976, Aff'g 402 F. Supp. 107 (1975).
3. Working Paper A., p. 23.
4. Ill. Rev. Stat. ch. 16½, par. 105, sec. 5(16), as amended by Public Act No. 81-841 (1979)
5. Working Paper A, pp. 23-24.
6. Ibid., pp. 26-30.
7. Ibid., p. 27.
8. Letter from Donald I. Baker, U.S. Assistant Attorney General, Department of Justice Antitrust Division, to William B. Brandt, pursuant to business review requested Mar. 7, 1977.
9. NETS requested and received a Business Review Letter from the Department of Justice which suggested that the mandatory sharing of Nebraska law and in turn NETS could be anticompetitive. As a result of this suggestion, NETS restructured itself but the law remains the same. (Sept. 30, 1981 letter to OTA from William H. Riley.)
10. *U.S.* v. *Rocky Mountain Automatic Clearinghouse Association*, Civil No. 77-A 319 (C.D.Colo. filed Apr. 27, 1972); *U.S.* v. *California Automatic Clearinghouse Association*, Civil No. 77-1643, filed May 6, 1977. *See* Working Paper A.
11. There are approximately 14,000 commercial banks, 4,850 savings and loan associations, 22,000 credit unions, and 470 mutual savings banks. *See* Working Paper A, p. 9. and *Moody's*, 1979.
12. For a discussion of this issue *see* Donn B. Parker, "The Potential Effects of Electronic Funds Transfer Systems on National Security," in Session 19, Applications of Communications Technology -Electronic Funds Transfer, of the International Conference on Computer Communications, Atlanta, Ga., 1980.

13. Working Paper A, p. 59; see also *The Report of the Commission on Postal Service*, April 1977.
14. Ibid.
15. Ibid., p. 60. *See also* "Automated Clearing House Network, Its Progress, Problems, Potential," *Banking*, March 1979.
16. Eger, "The Role of the Federal Reserve in Electronic Funds Transfer—An Executive Perspective," 25 Catholic University Law Rev. 139 (1976).
17. "Federal Reserve Options in Payment Mechanisms: A Summary," 62 Federal Reserve Bulletin 485 (1976); "Social Security Direct Deposit is only the Beginning," *Savings and Loan News* (July 1978), p. 66.
18. Working Paper A, p. 52. *See also*, Sept. 17, 1981 letter to OTA from Elliot C. McEntee of the Federal Reserve System.
19. *See* 58 Federal Reserve Bulletin, 1010, 1972: It is anticipated that the Federal Reserve System will install and manage a nationwide communications network through which interregional settlements between financial institutions will be made.
20. Public Law 96-221.
21. For a further discussion of arguments for and against continued Federal Reserve operation of ACH, including the privacy issue, *see* Working Paper D: Irvine Research Corp., *An Assessment of Equity and Privacy Issues in Electronic Funds Transfer* (September 1980), pp. 163-168.
22. Ibid., p. 167. *See also* Working Paper A: Imperial Computer Services, *Electronic Funds Transfer: The Policy Issues* (May 1979), pp. 48-51.

Appendix B

Working Papers

Working Paper A - Electronic Funds Transfer: The Policy Issues; Imperial Computer Services, Inc., May 1979

Working Paper B - EFT: The Next Fifteen Years; Electronic Banking, Inc., June 1980

Working Paper C - Societal Impacts of Future EFT Security Measures; ICS Group, Inc., September 1980

Working Paper D - An Assessment of Equity and Privacy Issues in Electronic Funds Transfer Systems; The Irvine Research Corporation, September 1980

Working Paper E - EFT - Description and Partial Evaluation; Daniel Kevin, November 1979

Working Paper F - A Review of Existing and Proposed Legislation as it Relates to EFT Privacy; Daniel Kevin, November 1979

Working Paper G - EFT System Integrity; Daniel Kevin, November 1979

Working Papers A, B, C, D, E, F, and G will be available from the National Technical Information Service (NTIS), U.S. Department of Commerce, Springfield, Va. Please contact OTA's Publishing Office (202) 224-8996 for availability dates and ordering information.

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an advisory arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts which can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects—both beneficial and harmful—of technological applications.

Requests for studies are made by chairmen of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a nonvoting member.

OTA currently has studies underway in nine general areas: energy, international security and commerce, materials, food and renewable resources, health, human resources, communication and information technologies, oceans and environment, and space technology.

OTA-BP-CIT-12

MARCH 1982